

UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF WASHINGTON  
AT SEATTLE

JESUS CASTILLO, MARK KNOWLES, ALEX  
RODRIGUEZ, NICHOLAS JAMES  
THROLSON, R.S., KIMBERLY SCOTT,  
ROBIN WARBEY, DANIEL SMITH, MATT  
GROVES, VERN DEOCHOA, TYRONE  
WASHINGTON, individually, and on behalf of  
those similarly situated,

Plaintiffs,

v.

COSTCO WHOLESALE CORPORATION, a  
Washington corporation,

Defendant.

NO. 2:23-cv-01548-JHC

**CONSOLIDATED COMPLAINT -  
CLASS ACTION**

**JURY TRIAL DEMANDED**

Plaintiffs Jesus Castillo, Mark Knowles, Alex Rodriguez, Nicholas James Throlson, R.S., Kimberly Scott, Robin Warbey, Daniel Smith, Matt Groves, Vern DeOchoa, and Tyrone Washington (“Plaintiffs”), individually and on behalf of all others similarly situated, by and through their attorneys of record, assert the following against Defendant Costco Wholesale Corporation (“Costco” or “Defendant”).

**INTRODUCTION**

1. This class action arises out of Costco’s unlawful use of third-party tracking technologies (the “Tracking Tools”) to disclose surreptitiously millions of Americans’ private

1 and protected communications, including their highly personal health information, to third  
 2 parties, all without these consumers' knowledge or consent. By purposely embedding and  
 3 deploying the Tracking Tools on Costco's Website, www.costco.com, Costco engages in the  
 4 unauthorized disclosure of its Pharmacy patients' highly sensitive Personal Health Information  
 5 ("PHI") and Personally Identifiable Information ("PII") (collectively "Sensitive Information") to  
 6 third parties, including, but not limited to, Meta Platforms, Inc. d/b/a/ Meta ("Facebook") and  
 7 Google.<sup>1</sup> Such conduct blatantly violates state and federal law.

8         2. As a multinational company, and one of the largest global retailers today,  
 9 Defendant operates a membership-only warehouse club that serves millions of customers  
 10 worldwide.<sup>2</sup> Defendant owns and controls the website www.costco.com and the subpages for its  
 11 pharmaceutical immunization services provided by Costco Pharmacy at  
 12 www.costco.com/pharmacy (collectively Defendant's "Website"). In its ordinary course of  
 13 business, Defendant encourages patients and prospective patients to use its Pharmacy subpages  
 14 of its Website to communicate about their prescriptions, research medications for purchase, order  
 15 new prescriptions, request refills for existing medications, inquire about specific immunizations,  
 16 search for local Medicare supplemental insurance, and more.<sup>3</sup> In doing so, Costco represents to  
 17 patients that its Website, which includes its Pharmacy webpages, is a secure platform and that

18  
 19 <sup>1</sup> At all relevant times, Costco is and was a "covered entity" under HIPAA because it is "[a] health care provider  
 20 who transmits any health information in electronic form in connection with a transaction covered" by HIPAA. 45  
 21 C.F.R. § 160.103. A HIPAA "health care provider" is "a provider of medical or health services" and "any other  
 22 person or organization who furnishes, bills, or is paid for health care in the normal course of business." *Id.* Moreover,  
 23 "health care" is defined under HIPAA as "care, services, or supplies related to the health of an individual" and  
 24 includes "[p]reventative, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling,  
 service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an  
 individual or that affects the structure or function of the body; and . . . [the s]ale or dispensing of drug, device,  
 equipment, or other item in accordance with a prescription." *Id.* Costco provides care, services, and supplies related  
 to the health of an individual, which includes Costco Pharmacy and its sale and dispensing of prescription  
 medications to patients and prospective patients.

25 <sup>2</sup> *Company Report: Cosco Wholesale Corp, Company Overview*, Bloomberg Law (Aug. 21, 2023).

26 <sup>3</sup> *See Create an account*, <https://mobilecontent.costco.com/live/resource/img/pharmacy-training/pharmacy-training.html#/lessons/w-E1ac5YoS4RPxcoQgAASNxFz9k6pcgN> (last visited Aug. 30, 2023) (encouraging patients to sign up for the Costco Mail Order option so that they can, "Fill your prescriptions online and have it mailed to your home.").

1 the information provided therein will remain protected and confidential. Yet Costco fails to  
 2 disclose that it shares patient online activities and personal health information via the Tracking  
 3 Tools.

4 3. One of the Tracking Tools Defendant deployed on its website is the Meta Pixel  
 5 (“Pixel”).<sup>4</sup> Pixel is a snippet of code that, when embedded on a website, tracks the website  
 6 visitor’s activity on that website and sends that data to a third party, like Meta. This includes  
 7 tracking and logging pages and subpages the website user visits during a website session that  
 8 reveal patient status and other personal identifying and protected health information, searches,  
 9 and other submissions to the website, which in many cases includes sensitive personal and  
 10 identifying information that is not anonymized. Indeed, Pixel is routinely used to target specific  
 11 customers by utilizing the data gathered through Pixel to build profiles for the purpose of future  
 12 targeting and marketing. Here, the information transmitted to third-party Meta without Plaintiffs’  
 13 consent included private health information,<sup>5</sup> which is some of the most personal and sensitive  
 14 data Plaintiffs have.

15 4. Additionally, when a patient communicates with Costco’s Website where Pixel is  
 16 present, Pixel source code causes the exact content of the patients’ communications with the  
 17 Website to be re-directed to Meta in a way that identifies the person as a patient. For example,  
 18 Plaintiffs are patients and prospective patients of Costco Pharmacy and, while receiving or  
 19 researching pharmaceutical care from Costco Pharmacy, used the Website to communicate about  
 20 ordering new prescriptions, requesting prescription refills, enrolling in automated prescription  
 21 services, viewing prescription history, new prescriptions, and prescription pricing, and  
 22

---

23 <sup>4</sup> Meta also provides other tracking technologies that give the same or similar tracking functionalities as Pixel,  
 including, but not limited to, Conversions API, SDKs, and Audiences.

24 <sup>5</sup> Under HIPAA, “health information” is defined as “any information[], whether oral or recorded in any form or  
 25 medium, that . . . [i]s created or received by a health care provider . . . and [r]elates to the past, present, or future  
 26 physical or mental health or condition of an individual; the provision of health care to an individual; or the past,  
 present, or future payment for the provision of health care to an individual.” 45 C.F.R. § 160.103. Additionally,  
 HIPAA defines “health care” as “care, services, or supplies related to the health of an individual” and includes, but  
 is not limited to, the “[s]ale or dispensing of drug, device, equipment, or other item in accordance with a  
 prescription.” *Id.*

1 conducting medication-related research. Unbeknownst to Plaintiffs and Class Members, when  
 2 they attempted to log-in to their patient accounts, searched for prescriptions and related pricing,  
 3 and inquired about immunizations, among other sensitive health-related topics, Pixel secretly  
 4 intercepted, recorded, and transmitted those private communications to Meta along with unique  
 5 identifiers Meta could use to identify the Class Members.

6 5. Defendant used Pixel to intercept its users' communications and have those  
 7 communications associated with Facebook user profiles for purposes of future ad targeting and  
 8 marketing.

9 6. As a result of Defendant's use of Pixel, Plaintiffs' and Class Members' Sensitive  
 10 Information, including, but not limited to, computer IP addresses; patient status; prescription  
 11 information (including specific drugs and pricing information); immunization information;  
 12 treatments; patient location; health insurance coverage; and unique identifiers used to link the  
 13 web communications to Plaintiffs and the Class, was compromised and disclosed to third parties  
 14 without authorization or consent.

15 7. Such private information would allow Meta to know that a specific patient was  
 16 seeking confidential pharmaceutical care or exploring drug therapy options for a specific  
 17 condition or had filled prescriptions for certain drugs (some of which may be associated with a  
 18 specific medical condition).

19 8. On information and belief, Defendant's Tracking Tools have also transmitted  
 20 patients' Sensitive Information to additional unauthorized third parties for marketing and  
 21 advertising purposes, including Google.

22 9. Google tracking technologies operate much like the Meta Pixel. As one District  
 23 Court recently described:

24 Whenever a user visits a website that is running Google Analytics, Ad Manager, or  
 25 some similar Google service, Google's software directs the user's browser to send  
 26 a separate communication to Google. This happens even when users are in private  
 browsing mode, unbeknownst to website developers or the users themselves. The  
 operation is not in dispute. When a user visits a website, the user's browser sends a  
 "GET" request to the website to retrieve it. This GET request contains the following

1 information: the Request URL, or the URL of the specific webpage the user is  
 2 trying to access; the user's IP address; the User-agent, which identifies the user's  
 3 device platform and browser; user's geolocation, if available; the Referer, which is  
 4 the URL of the page on which the user clicked a link to access a new page; event  
 5 data, which describes how users interact with a website, for example, whether they  
 6 saw an ad or played a video; and the actual search queries on the site. At the same  
 time, the user's browser reads Google's code, which is embedded on the website.  
 Google's code instructs the user's browser to send a second and concurrent  
 transmission directly to Google. This second transmission tells Google exactly  
 what a user's browser communicated to the website.<sup>6</sup>

7 10. In secretly deploying the Tracking Tools on its website to intercept website  
 8 communications concerning its patients' and prospective patients' PHI, Defendant acted with a  
 9 tortious and criminal purpose in violation of state and federal laws.

10 11. Plaintiffs and the Class Members never consented to, authorized, or otherwise  
 11 agreed to allow Defendant to disclose their Sensitive Information to anyone other than those  
 12 reasonably believed to be part of Costco acting in some healthcare-related capacity. Despite this,  
 13 Defendant knowingly and intentionally disclosed Plaintiffs' and the Class Members' Sensitive  
 14 Information to Meta, Google, and other potential third parties.

15 12. Given the nature of Meta and Google's businesses as two of the world's largest  
 16 online advertising companies, Plaintiffs' and the Class Members' Sensitive Information can and  
 17 will likely be further used by or exposed to additional third parties.

18 13. As a direct and proximate result of Defendant's unauthorized exposure of  
 19 Plaintiffs' and the Class Members' Sensitive Information, Plaintiffs and the Class Members have  
 20 suffered injury, including an invasion of privacy; conversion of their private and valuable PHI  
 21 for defendant's gain; loss of the benefit of the bargain Plaintiffs and the Class Members  
 22 considered at the time they bargained for pharmaceutical services and agreed to use Defendant's

23 \_\_\_\_\_  
 24 <sup>6</sup> *Brown v. Google LLC*, No. 4:20-CV-3664-YGR, 2023 WL 5029899, at \*2 (N.D. Cal. Aug. 7, 2023). As  
 25 explained by the Court in *Brown*, Google connects user data to IP addresses; IP addresses have been classified by  
 26 the United States Department of Health and Human Services ("HHS") as personally identifying information. Use  
 of Online Tracking Technologies by HIPAA Covered Entities and Business Associates, U.S. Dept of Health and  
 Hum. Servs. (Dec. 1, 2022), <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html>.

1 Website for services; statutory damages; and the continued and ongoing risk to their Sensitive  
2 Information.

3 14. Accordingly, Plaintiffs bring this action individually, and on behalf of a Class of  
4 similarly situated individuals, to recover for harms suffered and assert the following claims:  
5 Violations of Electronic Communications Privacy Act (“ECPA”) (18 U.S.C. § 2511); Violations  
6 of the Washington Privacy Act (Wash. Rev. Code § 9.73.030 *et seq.*); Violations of the  
7 Washington Consumer Protection Act (“WCPA”) (Wash. Rev. Code § 19.86 *et seq.*); Violations  
8 of the Washington Uniform Health Care Information Act (“UHCIA”) (Wash. Rev. Code. § 70.02  
9 *et seq.*); Violations of the California Invasion of Privacy Act, (Cal. Penal Code, § 630 *et seq.*);  
10 Violations of the California Confidentiality of Medical Information Act, (Cal. Civ. Code § 56 *et*  
11 *seq.*); Violation of the Florida Security of Communications Act (Florida Statutes § 934.01 *et*  
12 *seq.*); Invasion of Privacy; Breach of Implied Contract; Conversion; and Unjust Enrichment.

### 13 **PARTIES**

14 15. **Plaintiff Jesus Castillo** is a natural person domiciled in the State of California.  
15 At all relevant times, he resided in South El Monte, California. For the last several years, and  
16 most recently in 2022, he visited Defendant’s Website while residing in California to transfer his  
17 prescription medications from another pharmacy to Costco Pharmacy to purchase and refill his  
18 prescriptions with Costco. He communicated personal, private, and highly sensitive information  
19 while visiting Defendant’s Website. At all relevant times, Plaintiff Castillo had a Facebook  
20 account and generally remained logged into his account.

21 16. **Plaintiff Mark Knowles** is a natural person domiciled in the State of California.  
22 At all relevant times, he resided in Redondo Beach, California. For the last six years, and most  
23 recently in 2023, he visited Defendant’s Website while residing in California to enroll in Costco’s  
24 mail-in prescription order program; to order, view, and schedule monthly prescription refills; and  
25 to search for prescriptions and prescription pricing, including by utilizing the Website’s “search”  
26 bar. [REDACTED]

1 [REDACTED] He also visited  
 2 Defendant's Website to use the patient portal to order new prescriptions and request prescription  
 3 refills. He communicated personal, private, and highly sensitive information while visiting  
 4 Defendant's Website. At all relevant times, Plaintiff Knowles had a Facebook account and  
 5 generally remained logged in to his account.

6 17. **Plaintiff Alex Rodriguez** is a natural person domiciled in the State of California.  
 7 At all relevant times, he resided in Madera, California. For the last several years, and most  
 8 recently in 2023, he visited Defendant's Website while residing in California to order and view  
 9 new prescriptions and search for prescriptions and prescription pricing, including by utilizing the  
 10 Website's "search" bar. He also visited Defendant's Website to use the patient portal to order  
 11 new prescriptions, request prescription refills, review co-pay information, review prescription  
 12 pickup times, and communicate with pharmacists and technicians. He communicated personal,  
 13 private, and highly sensitive information while visiting Defendant's Website. At all relevant  
 14 times, Plaintiff Rodriguez had a Facebook account and generally remained logged in to his  
 15 account.

16 18. **Plaintiff Nicholas James Throlson** is a natural person domiciled in the State of  
 17 California. At all relevant times, he resided in Rialto, California. For the last two years, and most  
 18 recently in 2023, he visited Defendant's Website while residing in California to enroll in,  
 19 schedule, and view automatic prescription refill pickup and search for prescriptions and  
 20 prescription pricing, including by utilizing the Website's "search" bar. He also visited  
 21 Defendant's Website to use the patient portal to search for new prescriptions, review prescription  
 22 pricing, and assess whether to request prescription refills through Costco Pharmacy. [REDACTED]

23 [REDACTED] He  
 24 communicated personal, private, and highly sensitive information while visiting Defendant's  
 25 Website. At all relevant times, Plaintiff Throlson had a Facebook account and generally remained  
 26 logged in to his account. [REDACTED]

1 [REDACTED]  
2 [REDACTED]  
3 [REDACTED]  
4 19. **Plaintiff R.S.** is a natural person domiciled in the State of California, where he  
5 resided at all relevant times. As recently as 2023, R.S. visited Defendant's Website while  
6 residing in California to fill prescriptions, check the status of prescriptions, and to compare  
7 prescription prices using the Website's drug pricing tool. [REDACTED]  
8 [REDACTED]

9 [REDACTED] R.S. communicated personal, private, and highly sensitive information while  
10 visiting Defendant's Website. At all relevant times, Plaintiff R.S. had a Facebook account.

11 20. **Plaintiff Kimberly Scott** is a natural person domiciled in the State of California,  
12 where she resided at all relevant times. As recently as 2023, Plaintiff Scott visited Defendant's  
13 Website while residing in California to fill her prescriptions, [REDACTED]  
14 Plaintiff Scott communicated personal, private, and highly sensitive information while visiting  
15 Defendant's Website. At all relevant times, Plaintiff Scott had a Facebook account and generally  
16 remained logged in to her account.

17 21. **Plaintiff Robin Warbey** is a natural person domiciled in the State of California,  
18 where he resided at all relevant times. As recently as 2023, Plaintiff Warbey visited Defendant's  
19 Website while residing in California to search for [REDACTED]  
20 [REDACTED]

21 [REDACTED] Plaintiff Warbey communicated  
22 personal, private, and highly sensitive information while visiting Defendant's Website. At all  
23 relevant times, Plaintiff Warbey had a Facebook account and generally remained logged in to his  
24 account.

25 22. **Plaintiff Daniel Smith** is a natural person domiciled in the State of California,  
26 where he resided at all relevant times. As recently as 2023, Plaintiff Smith visited Defendant's  
Website while residing in California to refill prescriptions and purchase certain health

1 supplements. [REDACTED]

2 [REDACTED]

3 [REDACTED] Plaintiff Smith communicated personal, private, and highly sensitive information

4 while visiting Defendant's Website. At all relevant times, Plaintiff Smith had a Facebook account

5 and generally remained logged in to his account. [REDACTED]

6 [REDACTED]

7 [REDACTED]

8 23. **Plaintiff Matt Groves** is a natural person domiciled in the State of California,

9 where he resided at all relevant times. As recently as 2023, Plaintiff Groves visited Defendant's

10 Website while residing in California to check the status of and refill prescriptions [REDACTED]

11 [REDACTED]

12 [REDACTED]

13 Plaintiff Groves communicated personal, private, and highly sensitive information while visiting

14 Defendant's Website. At all relevant times, Plaintiff Groves had a Facebook account and

15 generally remained logged in to his account.

16 24. **Plaintiff Vern DeOchoa** is a natural person domiciled in the State of California,

17 where he resided at all relevant times. For approximately the last six years, Plaintiff Deochoa

18 has visited Defendant's Website while residing in California to check the status of and refill

19 prescriptions. [REDACTED]. Plaintiff DeOchoa communicated personal, private, and

20 highly sensitive information while visiting Defendant's Website. At all relevant times, Plaintiff

21 DeOchoa had a Facebook account and generally remained logged in to his account.

22 25. **Plaintiff Tyrone Washington** is a natural person domiciled in the State of

23 Florida, where he resided at all relevant times. Since approximately 2000, Plaintiff Washington

24 has been a customer of Costco and has fulfilled prescriptions through the Costco Website. Among

25 other medications, Plaintiff Washington has used the Costco website to fulfill prescriptions [REDACTED]

26 [REDACTED] At all

1 relevant times, Plaintiff Washington has maintained a Facebook account and generally remains  
 2 logged into that account. Plaintiff Washington received targeted Facebook ads from Defendant  
 3 following his visits to the Website as a result of Defendant's use of the Tracking Tools. Among  
 4 others, Plaintiff Washington recalls receiving advertisements for [REDACTED]

5 [REDACTED]  
 6 26. Plaintiffs reasonably expected that their online communications with Defendant  
 7 were between them and Defendant and that such communications would not be shared with third  
 8 parties without their consent.

9 27. By disclosing to third parties its patients' prescription medications through the  
 10 Tracking Tools, Defendant also revealed its patients' underlying health conditions, enabling  
 11 unauthorized third parties to monetize that data through ad retargeting.

12 28. **Defendant Costco Wholesale Corporation** is a Washington corporation, is  
 13 licensed to do business in the State of Washington, and has its principal place of business in  
 14 Issaquah, Washington. Defendant's registered agent is John Sullivan, located at 999 Lake Drive,  
 15 Issaquah, Washington, 98027-8990.

16 29. Defendant is a multinational retailer that operates a membership-only warehouse  
 17 club. With a corporate history that dates to 1976,<sup>7</sup> Defendant is one of the largest retailers in the  
 18 world today, with more than 300,000 employees and serving millions of members and non-  
 19 members around the globe.<sup>8</sup> Defendant sells food, automotive, supplies, toys, hardware, sporting  
 20 goods, jewelry, electronics, apparel, health, and beauty aids, as well as other goods.<sup>9</sup> Costco also  
 21 offers pharmaceutical services through the Costco Pharmacy and the Pharmacy webpage.

22  
 23  
 24 <sup>7</sup> Robert Lewis, *Costco*, Britannica, <https://www.britannica.com/topic/Costco> (last visited Sept. 15, 2023).

25 <sup>8</sup> *About Us*, Costco Wholesale, <https://www.costco.com/about.html> (last visited Sept. 15, 2023); *Company Profile*,  
 Costco Wholesale, <https://investor.costco.com/company-profile/default.aspx> (last visited Sept. 15, 2023).

26 <sup>9</sup> *About Us*, Costco Wholesale, <https://www.costco.com/about.html> (last visited Sept. 15, 2023, 2023); *Overview of Costco Wholesale Corp (COST US Equity)*, Bloomberg Law, <https://www.bloomberglaw.com/company/ticker/COST%20US%20Equity> (last visited Sept. 15, 2023); *Costco*, Wikipedia, [https://en.wikipedia.org/wiki/Costco#See\\_also](https://en.wikipedia.org/wiki/Costco#See_also) (last visited Sept. 15, 2023); *Company Profile*, Costco Wholesale, <https://investor.costco.com/company-profile/default.aspx> (last visited Sept. 15, 2023).



1 website visit sessions initiated by Costco's customers located throughout the United States,  
2 including in Washington, and the claims alleged herein arise from those activities.

3 36. Costco also knows that many patients and prospective patients visit and interact  
4 with Costco Website while they are physically present in Washington and throughout the United  
5 States and its territories. Both desktop and mobile versions of Costco's Website allow a user to  
6 search for nearby Costco warehouses to schedule appointments for immunizations and  
7 vaccinations,<sup>11</sup> enroll in prescription refill pickup at limited Costco Pharmacy warehouse  
8 locations,<sup>12</sup> enroll in direct-mail prescription delivery,<sup>13</sup> search pricing and information regarding  
9 prescription and over-the-counter medications,<sup>14</sup> and locate nearby Medicare insurance<sup>15</sup> by  
10 providing the user's "current location," or by selecting "my warehouse" and "my delivery  
11 location," as furnished by the location-determining tools of the device the user is using, by the  
12 user's IP address (*i.e.*, without requiring the user to manually input an address), or by a user's  
13 manual entry.<sup>16</sup>

14 37. Through its Website, which included the Tracking Tools and was accessible to all  
15 Washington residents, Costco allowed consumers to view and interact with its marketed and  
16 advertised pharmaceutical services, directly engage with those services, exchange  
17 communications with the retailer, and create online accounts. Thus, users' employment of  
18 automatic location services in this way means that Costco is continuously made aware that people  
19 located throughout the United States, including in Washington, visit and interact with its Website  
20

21 <sup>11</sup> *Immunizations*, Costco Pharmacy, <https://www.costco.com/pharmacy/adult-immunization-program.html> (last  
22 visited Aug. 22, 2023).

23 <sup>12</sup> *Costco RX Locker: Prescription Pickup*, Costco Pharmacy, chrome-  
24 extension://efaidnbmnnnibpcajpegclclefindmkaj/[https://mobilecontent.costco.com/live/resource/img/static-us-  
25 landing-pages/pharmacy\\_pickup.pdf](https://mobilecontent.costco.com/live/resource/img/static-us-landing-pages/pharmacy_pickup.pdf) (last accessed Aug. 22, 2023); *Refill Now*, Costco Pharmacy,  
26 <https://costco.web.medrefill.com/csweb/#/refill> (last visited Aug. 22, 2023).

<sup>13</sup> *About Prescription Mail Order*, Costco Pharmacy, <https://www.costco.com/pharmacy/about-home-delivery.html>  
27 (last visited Aug. 22, 2023); Costco Pharmacy, [https://mobilecontent.costco.com/live/resource/img/pharmacy-  
28 training/pharmacy-training.html#lessons/w-E1ac5YoS4RPxcoQgAASNXFz9k6pcgN](https://mobilecontent.costco.com/live/resource/img/pharmacy-training/pharmacy-training.html#lessons/w-E1ac5YoS4RPxcoQgAASNXFz9k6pcgN) (last visited Aug. 22, 2023).

<sup>14</sup> *Member Prescription Program*, Costco Pharmacy, <https://www.costco.com/cmpp> (last visited Aug. 22, 2023).

<sup>15</sup> *Medicare Plan Finder*, Costco Pharmacy, <https://www.costco.com/pharmacy/medicare.html> (last visited Aug. 22,  
29 2023).

<sup>16</sup> *Find a Store*, Costco Pharmacy, <https://costco.web.medrefill.com/csweb/#/store> (last visited Aug. 22, 2023).

1 and services made available by Costco, and that such website visitors are being wiretapped in  
2 violation of federal and state law.

3 38. Venue is proper under 28 U.S.C. §§ 1391(b)(1) – (2) because Defendant’s  
4 principal place of business is in this District and because a substantial part of the events,  
5 omissions, and acts giving rise to the claims herein occurred in this District.

### 6 **FACTUAL ALLEGATIONS**

#### 7 **A. Federal Regulators Have Warned Healthcare Providers About the Use of Tracking** 8 **Technologies**

9 39. The surreptitious collection and disclosure of Sensitive Information is an  
10 extremely serious data security and privacy issue. Both the Federal Trade Commission (“FTC”)  
11 and the Office for Civil Rights of the U.S. Department of Health and Human Services (“HHS”)  
12 have recently reiterated the necessity for data security and privacy concerning health information.

13 40. For instance, the FTC recently published a bulletin entitled *Protecting the privacy*  
14 *of health information: A baker’s dozen takeaways from FTC cases*, in which it noted that  
15 “[h]ealth information is not just about medications, procedures, and diagnoses. Rather, it is  
16 anything that conveys information—or enables an inference—about a consumer’s health. Indeed,  
17 [recent FTC enforcement actions involving] Premom, BetterHelp, GoodRx and Flo Health make  
18 clear that the fact that a consumer is using a particular health-related app or website—one related  
19 to mental health or fertility, for example—or how they interact with that app (say, turning  
20 ‘pregnancy mode’ on or off) may itself be health information.”<sup>17</sup>

21 41. The FTC is unequivocal in its stance as it informs—in no uncertain terms—  
22 companies that provide healthcare services that they should not use tracking technologies to  
23 collect sensitive health information and disclose it to various platforms without informed  
24 consent:

25 \_\_\_\_\_  
26 <sup>17</sup> See Elisa Jillison, *Protecting the privacy of health information: A Baker’s dozen takeaways from FTC cases*, the  
FTC Business Blog (July 25, 2023), <https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases> (last visited Jan. 18, 2024).

**Don't use behind-the-scenes tracking technologies that contradict your privacy promises or otherwise harm consumers.** In today's surveillance economy, the consumer is often the product. Consumer data powers the advertising machine that goes right back to the consumer. But when companies use consumers' sensitive health data for marketing and advertising purposes, such as by sending that data to marketing firms via tracking pixels on websites or software development kits on apps, watch out. [Recent FTC enforcement actions such as] *BetterHelp*, *GoodRx*, *Premom*, and *Flo* make clear that practices like that may run afoul of the FTC Act if they violate privacy promises or if the company fails to get consumers' affirmative express consent for the disclosure of sensitive health information.<sup>18</sup>

42. In December 2022, HHS similarly warned healthcare providers that, "Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules."<sup>19</sup> The OCR's guidance also made clear that, "disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures."<sup>20</sup>

43. The HHS guidance further warned that "Tracking technologies on a regulated entity's unauthenticated webpage that addresses specific symptoms or health conditions, such as pregnancy or miscarriage, or that permits individuals to search for doctors or schedule appointments without entering credentials may have access to PHI in certain circumstances."<sup>21</sup> For example, "tracking technologies could collect an individual's email address and/or IP address when the individual visits a regulated entity's webpage to search for available appointments with a health care provider," in which case the "regulated entity is disclosing PHI to the tracking technology vendor, and thus the HIPAA Rules apply."<sup>22</sup>

<sup>18</sup> *Id.* (emphasis added).

<sup>19</sup> *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html>

<sup>20</sup> *Id.*

<sup>21</sup> *Id.*

<sup>22</sup> *Id.*

44. In July 2023, the FTC and HHS sent a letter to approximately 130 healthcare providers warning them about the use of online tracking technologies that could result in unauthorized disclosures of Sensitive Information to third parties.<sup>23</sup> The letter highlighted the “risks and concerns about the use of technologies, such as the Meta/Facebook pixel and Google Analytics, that can track a user’s online activities,” and warned about “[i]mpermissible disclosures of an individual’s personal health information to third parties” that could “result in a wide range of harms to an individual or others.”<sup>24</sup> According to the letter, “[s]uch disclosures can reveal sensitive information including health conditions, diagnoses, medications, medical treatments, frequency of visits to health care professionals, where an individual seeks medical treatment, and more.”<sup>25</sup>

#### **B. Defendant Collected, Maintained, and Stored Sensitive Information**

45. Despite these clear warnings from federal regulators, Defendant Costco embedded Tracking Tools on its pharmacy webpage to secretly track its patients’ communications regarding healthcare and prescription information and disclose those communications to third parties.

46. To obtain pharmaceutical services from Defendant, individuals, like Plaintiffs and members of the Class, must provide Defendant with highly sensitive information, including PHI, PII, or both. Defendant compiles, stores, and maintains the highly valuable and sensitive PHI and/or PII and, often, through the provision of its services, creates records containing additionally highly sensitive and valuable data concerning patients’ computer IP addresses, patient status, prescription information (including specific drugs and pricing information), immunization information, treatments, patient location, health insurance coverage, and unique identifiers used to link the web communications to Plaintiffs and the Class. Defendant serves millions of

<sup>23</sup> <https://www.ftc.gov/business-guidance/blog/2023/07/ftc-hhs-joint-letter-gets-heart-risks-tracking-technologies-pose-personal-health-information>

<sup>24</sup> [https://www.ftc.gov/system/files/ftc\\_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf)

<sup>25</sup> *Id.*

1 individuals each year, meaning it creates and maintains a massive repository of Sensitive  
2 Information.

3 47. Defendant tells patients it will keep their Sensitive Information secure and private.  
4 Indeed, Defendant maintains a Privacy Policy, stating, “[R]est assured that here at Costco, we  
5 absolutely respect your right to privacy. Costco collects, uses[,] and shares your personal  
6 information in accordance with Your Privacy Rights.”<sup>26</sup> This Policy further provides that Costco  
7 takes “reasonable and appropriate steps to help protect personal information from unauthorized  
8 access, use, disclosure . . .”<sup>27</sup>

9 48. In its Notice of Patient’s Rights, Defendant confirms that its patients have the  
10 right “[t]o have the patient’s pharmaceutical records maintained in a[] . . . confidential manner.”<sup>28</sup>

11 49. Costco Pharmacy affirms it “respects [each patient’s] right to privacy” and  
12 reassures it maintains its “patient profile database separately from other Costco records to  
13 safeguard the confidentiality of personal pharmacy information.”<sup>29</sup>

14 50. Defendant’s Notice of Privacy Practices<sup>30</sup> acknowledges that Costco is “required  
15 by law to maintain the privacy and security of [its patients’] PHI.”<sup>31</sup> The Notice further states  
16 that “[t]o protect the privacy of PHI, [Costco] limit[s] the way PHI is used or disclosed to  
17 others”<sup>32</sup> and acknowledges Costco’s obligation to “obtain . . . written authorization” before a  
18

19 <sup>26</sup> *What is Costco’s Privacy Policy?*, Costco Wholesale, [https://customerservice.costco.com/app/answers/detail/a\\_id/1163/~/what-is-costcos-privacy-policy%3F](https://customerservice.costco.com/app/answers/detail/a_id/1163/~/what-is-costcos-privacy-policy%3F) (last visited Sept. 14, 2023).

20 <sup>27</sup> *Costco Wholesale Corporation Your Privacy Rights (United States and Puerto Rico)*, Costco Wholesale, <https://www.costco.com/privacy-policy.html> (last updated June 20, 2023) (last visited Sept. 14, 2023).

21 <sup>28</sup> *Notice of Patient’s Rights*, Costco Pharmacy, <https://www.costco.com/pharmacy/about-home-delivery.html#patient-rights> (last visited on Sept. 14, 2023).

22 <sup>29</sup> *Confidentiality of Personal Pharmacy Information*, Costco Pharmacy, <https://www.costco.com/pharmacy/about-home-delivery.html#confidentiality> (last visited Sept. 14, 2023).

23 <sup>30</sup> The Costco Health Centers Notice of Privacy Practices is specific to health information handled by Costco Pharmacy as it “applies to PHI created, received, maintained or transmitted by or on behalf of Costco Pharmacies, Costco Optical Centers, and Costco Hearing Aid Centers (the ‘Costco Health Centers’).”

24 <sup>31</sup> *Costco Health Centers Notice of Privacy Practices* (Jan. 1, 2019), at 1, <chrome-extension://efaidnbmnnnipccpgcglefindmkaj/https://www.costco.com/wcsstore/CostcoUSBCCatalogAssetStore/rx/HIPAA-Privacy-Practice-19.pdf> (last visited Sept. 14, 2023). Costco’s Notice provides that PHI relates to (1) a patient’s physical or mental condition, (2) the provision of health care services to the patient, or (3) payment for a patient’s health care, and that this could include a patient’s “prescriptions” and “information [] provide[d] on any Costco Health Center patient health history form.” *Id.*

26 <sup>32</sup> *Id.*

1 patient's PHI is used or disclosed for any purpose other than that listed in the Notice, including  
 2 for marketing or "payment in exchange for providing [a patient's] PHI" to a third party.<sup>33</sup>

3 51. Plaintiffs and the Class Members had a reasonable expectation of privacy and  
 4 relied on Defendant to protect the Sensitive Information provided to it and created by it,  
 5 especially because pharmacists and other health care practitioners and their facilities are required  
 6 to maintain confidentiality of patient records, with very limited exceptions. Defendant knew or  
 7 should have known that failing to protect patient information adequately could cause substantial  
 8 harm by exposing patient data to unauthorized third parties, causing a loss of privacy and loss of  
 9 control over patients' personal information. Moreover, through its various policies, Defendant  
 10 acknowledged its obligation to safeguard sensitive information reasonably against unauthorized  
 11 disclosure of such information to third parties, like Meta.

12 52. A privacy violation of this type, in which Defendant intentionally granted access  
 13 to third parties to record and collect information on the company's systems, collect user data,  
 14 including Sensitive Information and highly confidential medical records without restriction,  
 15 could not occur but for Defendant's blatant disregard for patient privacy.

16 53. Defendant violated several basic privacy and data standards regarding patient  
 17 privacy and confidentiality.

18 54. As described throughout this Complaint, Defendant did not reasonably protect,  
 19 secure, or store Plaintiffs' and the Class Members' Sensitive Information, but rather intentionally  
 20 and knowingly granted third parties access to confidential information that it knew or should  
 21 have known was unlawful.

22 55. Defendant deprived Plaintiffs and the Class Members of their privacy rights when  
 23 it (i) installed the Tracking Tools on its Website and thereby surreptitiously intercepted, tracked,  
 24 recorded, and disclosed Plaintiffs' and other online patients' personal and private  
 25 communications and information; (ii) disclosed Plaintiffs' and the Class Members' protected  
 26

---

<sup>33</sup> *Id.* at 4.

1 information to unauthorized third parties; and (iii) and undertook this pattern of conduct without  
 2 notifying—and without obtaining the express written consent of—Plaintiffs and the Class  
 3 Members.

4 56. Consequently, Meta, Google, and potentially other third parties, obtained access  
 5 to and collected confidential patient data without the patients' authorization, resulting in a  
 6 significant invasion of patient privacy and disclosure of sensitive data.

### 7 **C. The Meta Pixel**

8 57. Through its Website, Defendant connects Plaintiffs and the Class Members to  
 9 Defendant's digital health care platform with a core goal of increasing profitability.

10 58. In furtherance of that goal, and to increase the success of its advertising and  
 11 marketing, Defendant purposely embedded and deployed Meta Pixel on its Website. By doing  
 12 so, Defendant surreptitiously shared its patients' and prospective patients' identities and online  
 13 activity, including private communications and search results related to past and current  
 14 prescription medications, treatments, immunizations, health insurance coverage, and other  
 15 Sensitive Information, with Meta.

16 59. Meta's core business function is to sell advertising, and it does so on several  
 17 platforms, including Facebook and Instagram. The bulk of Meta's billions of dollars in annual  
 18 revenue comes from advertising—a practice in which Meta actively participates by using  
 19 algorithms that approve and deny ads based on the ads' content, human moderators that further  
 20 review ads for both legality and aesthetics prior to and after the ads are published, and other  
 21 algorithms that connect ads to specific users, without the assistance or input of the advertiser.

22 60. Over the last decade, Facebook, now Meta, has become one of the largest and  
 23 fastest growing online advertisers in the world. Since its creation in 2004, Facebook's daily,  
 24 monthly, and annual user base has grown exponentially to billions of users.

25 61. Meta's advertising business has been successful due, in significant part, to Meta's  
 26 ability to target users, both based on information users provide to Meta, and based on other

1 information about users Meta extracts from the Internet at large. Given the highly specific data  
 2 used to target particular users, thousands of companies and individuals utilize Facebook's  
 3 advertising services.

4 62. One of Meta's most powerful advertising tools is the "Meta Pixel" (formerly the  
 5 "Facebook Pixel"), which it first launched in 2015.

6 63. Meta branded Pixel as "a new way to report and optimize for conversions, build  
 7 audiences and get rich insights about how people use your website." Meta further stated:

8 Facebook pixel, [is] a new way to report and optimize for conversions, build  
 9 audiences[,] and get rich insights about how people use your website. We're also  
 10 announcing the availability of custom conversions, a new rule-based method to  
 track and report conversions for your Facebook ads.

11 Facebook pixel makes things simple for advertisers by combining the  
 12 functionality of the Conversion Tracking pixels and Custom Audience pixels into  
 a single pixel. You only need to place a single pixel across your entire website to  
 13 report and optimize for conversions. Since it is built on top of the upgraded  
 Custom Audience pixel, all the features announced in our previous blog post  
 (Announcing Upgrades to Conversion Tracking and Optimization at Facebook)  
 14 are supported through Facebook pixel as well.

15 [Advertisers and website operators] can use Facebook pixel to track and optimize  
 for conversions by adding standard events (*e.g.*, Purchase) to your Facebook pixel  
 16 base code on appropriate pages (*e.g.*, purchase confirmation page).<sup>34</sup>

17 64. Pixel is an easily attainable piece of code that Meta makes available to website  
 18 developers for free. In exchange, at a minimum, website developers must agree to Meta's  
 Business Tool Terms.<sup>35</sup>

19 65. The Business Tool Terms note that the Meta's Business Tools, including Pixel,  
 20 will capture two types of information: "Contact Information" which "personally identifies  
 21  
 22  
 23

24 <sup>34</sup> Cecile Ho, *Announcing Facebook Pixel*, Meta (Oct. 14, 2015), <https://developers.facebook.com/ads/blog/post/v2/2015/10/14/announcing-facebook-pixel/> (last visited Sept. 14, 2023).

25 <sup>35</sup> See Meta Business Tool Terms,  
 26 [https://www.facebook.com/legal/businesses/paipv=0&eav=AfaHqYwiwGYZ0X0vZZ1I5uQ1zuI0STn-VURAyVhvlzw1Df5nxIgiuXOqcd5A8yKuEtk&\\_rdr](https://www.facebook.com/legal/businesses/paipv=0&eav=AfaHqYwiwGYZ0X0vZZ1I5uQ1zuI0STn-VURAyVhvlzw1Df5nxIgiuXOqcd5A8yKuEtk&_rdr) ("When you use any of the Meta Business Tools . . . or otherwise enable the collection of Business Tool Data . . . these Business Tool Terms govern the use of that data") (last visited Jan. 22, 2024).

1 individuals,” and “Event Data” which contains additional information about people and their use  
 2 of a developer’s website.<sup>36</sup>

3 66. The Business Tools Terms also require websites to “provide[] robust and  
 4 sufficiently prominent notice to users . . . on each web page where our pixels are used that links  
 5 to a clear explanation (a) that third parties, including Meta, may . . . collect or receive information  
 6 from your websites and elsewhere on the Internet and use that information to . . . deliver ads, (b)  
 7 how users can opt out of the collection and use of information . . . and (c) where a user can access  
 8 a mechanism for exercising such choice[.]”<sup>37</sup>

9 67. However, even with all of these protocols in place, Meta flatly prohibits the  
 10 disclosure of Business Tool Data “that you know or reasonably should know . . . includes health,  
 11 financial information or other categories of sensitive information (including any information  
 12 defined as sensitive under applicable laws, regulations and applicable industry guidelines).”<sup>38</sup>

13 68. After agreeing to the Business Tools Terms, website developers can choose to  
 14 install and use Pixel on their websites to track and measure certain actions, such as a website  
 15 visitor’s text searches and page views, including the detailed URLs triggered by page views.  
 16 When a website visitor takes an action a developer chooses to track on its website, Pixel is  
 17 triggered and sends data about that “Event” to Meta. All of this happens without the user’s  
 18 knowledge or consent.

19 69. Web browsers are software applications that allow consumers to navigate the web  
 20 and view and exchange electronic information and communications over the Internet. Each  
 21 “client device” (such as a computer, tablet, or smart phone) accesses web content through a web  
 22 browser (*e.g.*, Google’s Chrome browser, Mozilla’s Firefox browser, Apple’s Safari browser,  
 23 and Microsoft’s Edge browser).

24  
 25 

---

<sup>36</sup> *Id.* at Section 1(a)(i)-(ii)

26 <sup>37</sup> *Id.* at Section 3(c)(i)

<sup>38</sup> *Id.* at Section 1(h).

1           70. Every website is hosted by a computer “server” that holds the website’s contents  
 2 and through which the entity in charge of the website exchanges communications with Internet  
 3 users’ client devices via their web browsers.

4           71. Ultimately, a browsing session online may consist of thousands of web  
 5 communications. Web communications consist of HTTP or HTTPS Requests and HTTP or  
 6 HTTPS Responses, and any given browsing session may consist of thousands of individual  
 7 HTTP Requests and HTTP Responses, along with corresponding cookies:

- 8           • An **HTTP Request** is an electronic communication a website visitor sends from  
 9 his device’s browser to the website’s server. There are two types of HTTP  
 10 Requests: (1) GET Requests, which are one of the most common types of HTTP  
 11 Requests—in addition to specifying a particular URL (*i.e.*, web address), GET  
 12 Requests can also send data to the host server embedded inside the URL, and can  
 13 include cookies; and (2) POST Requests which can send a large amount of data  
 14 outside of the URL. In this case, a patient’s HTTP Request would be asking  
 15 Defendant’s Website to get certain information, such as a list of clinic locations  
 16 or prescriptions. So that servers can better understand what information users are  
 17 requesting, HTTP Requests also use URLs that contain parameters, which use  
 18 variables and assigned values in the URL to pass additional information through  
 19 the HTTP Request.
- 20           • **Cookies** are a text file that website operators and others use to store information  
 21 on the website visitor’s device; these can later be communicated to a server or  
 22 servers. Cookies are sent with HTTP Requests from website visitor’s devices to  
 23 the host server. Some cookies are “third-party cookies,” which means they can  
 24 store and communicate data when visiting one website to an entirely different  
 25 website. Third-party cookies are created by a website with a domain name other  
 26

than the one the user is visiting, in this case Meta.<sup>39</sup> There are also “first-party cookies,” like the fbp cookie, which is created by the website the user is visiting, in this case Defendant.<sup>40</sup> Meta uses both first- and third-party cookies in Pixel to link Facebook IDs and Facebook profiles, and Defendant sends these identifiers to Meta.

- An **HTTP Response** is a response to an HTTP Request. It is an electronic communication that is sent as a reply to the website visitor’s device’s web browser from the host server. HTTP responses may consist of a web page, another kind of file, text information, or error codes, among other data. Basically, the HTTP Response is when the website sends the requested information (*see* the HTTP Request); this is sometimes called the “Markup.”

72. A user’s HTTP Request essentially asks the Defendant’s Website to retrieve certain information (such as “Drug Pricing”). The HTTP Response then renders or loads the requested information in the form of Markup (i.e., the pages, images, words, buttons, and other features that appear on the patient’s screen as they navigate Defendant’s Website).

73. Every website, including Defendant’s, is composed of Markup and “Source Code.” Source code is a set of instructions that commands the website visitor’s browser to take certain actions when the web page loads or when a specified event triggers the code.

74. Source code may also command a web browser to transmit data to third parties in the form of an HTTP Request. Such data transmissions allow a website to export data about users and their actions to third parties. Third parties receiving this data are typically configured to track user data and communications for marketing purposes.

<sup>39</sup> *Third-Party Cookie*, PCMAG.com, <https://www.pcmag.com/encyclopedia/term/third-party-cookie> (last visited Sept. 14, 2023). This is also confirmable using web developer tools to inspect a website’s cookies and track network activity. This is confirmable by tracking network activity.

<sup>40</sup> *First-Party Cookie*, PCMAG.com, <https://www.pcmag.com/encyclopedia/term/first-party-cookie> (last visited Sept. 14, 2023). This is also confirmable using web developer tools to inspect a website’s cookies and track network activity.

1           75.     Transmission of a such data can be done quietly in the background without  
 2 notifying the web browser's user. The pixels are invisible to website users and thus, without any  
 3 knowledge, authorization, or action by the user, the website site developer (or website  
 4 commander) can use its source code to contemporaneously and to invisibly re-direct the user's  
 5 PII and other non-public medical information to third parties. Through Pixel, Defendant uses  
 6 source code that can accomplish just that.

7           76.     Pixel "tracks the people and the types of actions they take."<sup>41</sup> According to Meta,  
 8 Pixel is a piece of code that allows Defendant to measure the effectiveness of [its] advertising by  
 9 understanding the actions [website visitors] take on [its] website."<sup>42</sup> Thus, by secretly recording  
 10 and transmitting data to Meta—without the user's knowledge or consent—Pixel acts much like  
 11 a traditional wiretap controlled by Defendant.

12           77.     Through this online tracking technology, Meta intercepts each page a user visits,  
 13 what buttons they click, as well as the specific information the user inputs into the website and  
 14 other searches conducted. Pixel sends each of these pieces of information to Meta with PII, such  
 15 as the user's IP address. Meta stores this data on its own servers, in some instances for years on  
 16 end, and independently uses the data for its own financial gain.

17           78.     Importantly, this data is often associated with the individual user's Facebook  
 18 account. For example, if the user is logged into their Facebook account when the user visits  
 19 Defendant's website, Meta receives third-party cookies allowing Meta to link the data collected  
 20 by Pixel to the specific Facebook user. In other words, a user's personal and private information  
 21 sent by the Meta Pixel to Facebook is sent alongside that user's personal identifiers, including IP  
 22 address and cookie values, which can be linked to the user's unique Facebook account.

23           79.     Meta accomplishes this by placing cookies in the web browsers of users logged  
 24 into their services, which aids Meta in identifying users.

25  
 26 <sup>41</sup> *Retargeting*, Facebook, <https://www.facebook.com/business/goals/retargeting> (last visited Sept. 14, 2023).

<sup>42</sup> *About Meta Pixel*, Meta Business Help Center, <https://www.facebook.com/business/help/742478679120153?id=1205376682832142> (last visited Sept. 14, 2023).

80. One such example is the “c\_user” cookie, which is a type of third-party cookie assigned to each person who has a Facebook account. The “c\_user” cookie contains a numerical value known as the Facebook ID (“FID”) that uniquely identifies a Facebook user. It is composed of a unique and persistent set of numbers. A user’s FID is linked to their Facebook profile, which generally contains a wide range of demographic and other information about the user, including pictures, personal interests, work history, relationship status, and other details. Because the user’s Facebook Profile ID uniquely identifies an individual’s Facebook account, Meta—or any ordinary person—can easily use the Facebook Profile ID to quickly, and easily, locate, access, and view the user’s corresponding Facebook profile. Thus, when a Facebook user visits Defendant’s Website while logged in to their Facebook account, Pixel transmits the user’s private web communications with the Defendant along with the “c\_user” cookie. Meta can then use this information to match the web communications with the user’s Facebook ID.

81. Even if a user does not have a Facebook account or is not logged in to Facebook when browsing the Defendant’s Website, Pixel transmits the user’s web communications with Defendant’s Website to Meta along with a unique identifier associated with another cookie called the “\_fbp” cookie. Meta can then use that unique identifier to link the user’s web communications with the user’s Facebook ID. And if a user who does not have a Facebook account later creates an account, Meta may be able to associate the user’s historical browsing history intercepted via Pixel and “\_fbp” cookie to the newly created account.

82. Meta’s Business Tools Terms make clear that Pixel is meant to “match the Contact Information” of users “against user IDs . . . as well as to combine those user IDs with corresponding Event Data.”<sup>43</sup>

83. After Meta is finished processing users’ intercepted information, it makes the relevant analytics available to Costco through Meta’s Event Manager tool.

<sup>43</sup> Meta Business Tool Terms, Section 2(a)(i)(1), [https://www.facebook.com/legal/business/tech?paipv=0&eav=AfaHqYwiwGYZ0X0vZZ1I5uQ1zuI0STn-VURAYVhvlzw1Df5nxIgiuXOqcd5A8yKuEtk&\\_rdr](https://www.facebook.com/legal/business/tech?paipv=0&eav=AfaHqYwiwGYZ0X0vZZ1I5uQ1zuI0STn-VURAYVhvlzw1Df5nxIgiuXOqcd5A8yKuEtk&_rdr) (last visited Jan. 22, 2024).

84. Using the Events Manager, Costco can and is intended to review a summary of users' activity, including the pages, parameters and URLs sent through Pixel,<sup>44</sup> as well as any included metadata.<sup>45</sup>

85. Thus, without any knowledge, authorization, or action by a user, a website owner like Defendant can use its Source Code to commandeer the user's computing device, causing the device to re-direct the users' communications contemporaneously and invisibly to Meta. Meta then uses the information transmitted by Pixel to match the user with their Facebook ID.

86. Judge William H. Orrick on the U.S. District Court for the Northern District of California summarized how this process plays out:

To understand how the Meta Pixel typically works, imagine the following scenario. A shoe company wishes to gather certain information on customers and potential customers who visit its website. The shoe company first agrees to Meta's Business Tools Terms (discussed below), which govern the use of data from the Pixel. The shoe company then customizes the Meta Pixel to track, say, every time a site visitor clicks on the "sale" button on its website, which is called an "Event." Every time a user accesses the website and clicks on the "sale" button (i.e., an "Event" occurs), it triggers the Meta Pixel, which then sends certain data to Meta. Meta will attempt to match the customer data that it receives to Meta users—Meta cannot match non-Meta users. The shoe company may then choose to create "Custom Audiences" (i.e., all of the customers and potential customers who clicked on the "sale" button) who will receive targeted ads on Facebook, Instagram, and publishers within Meta's Audience Network. Meta may also provide the shoe company with de-identified, aggregated information so the shoe company understands the impact of its ads by measuring what happens when people see them. Meta does not reveal the identity of the matched Meta users to the shoe company.

*In re Meta Pixel Healthcare Litig.*, No. 22-CV-03580-WHO, 2022 WL 17869218, at \*2 (N.D. Cal. Dec. 22, 2022) (internal citations omitted).<sup>46</sup>

<sup>44</sup> *How to view pages, parameters and URLs in Meta Events Manager*,

<https://www.facebook.com/business/help/815029860145251> ("In Meta Events Manager, you can see a summary of pages, parameters and URLs recently sent through the Meta Pixel . . .") (last visited Jan. 22, 2024).

<sup>45</sup> A web developer using the Events Manager can "[c]lick on the filter icon to select what activity types and details are display." Developers can sort by activity types, including "automatically logged pixel events," which may contain metadata. *Test your app or web browser events using the test events tool*, <https://www.facebook.com/business/help/2040882565969969?id=1205376682832142> (last visited Jan. 22, 2024).

<sup>46</sup> In describing Pixel technology in *In re Meta Pixel Healthcare Litig.*, the court referenced the declaration of expert Richard M. Smith, which provides further details on the manner in which the challenged Pixel technology works and Meta's arrangements with health providers that employ it. 2022 WL 17869218, at \*2. *See* Declaration of Richard M. Smith, filed in *In re Meta Pixel Healthcare Litig.*, No. 22-CV-03580-WHO (N.D. Cal.) [ECF 49].

1 87. Pixel also allows a company, like Defendant, to impact the delivery of ads,  
 2 measure cross-device conversions, create custom audiences, and save money on advertising and  
 3 marketing costs.<sup>47</sup> But, most relevant here, Pixel allowed Defendant and Meta to track website  
 4 users secretly on Defendant's Website and intercept their communications with Defendant.

5 88. When visitors to Defendant's Website, like Plaintiffs and the Class Members,  
 6 communicated with Defendant or inquired about personal health-related topics and specific drug  
 7 prescriptions, that information was transmitted to and intercepted by Meta.

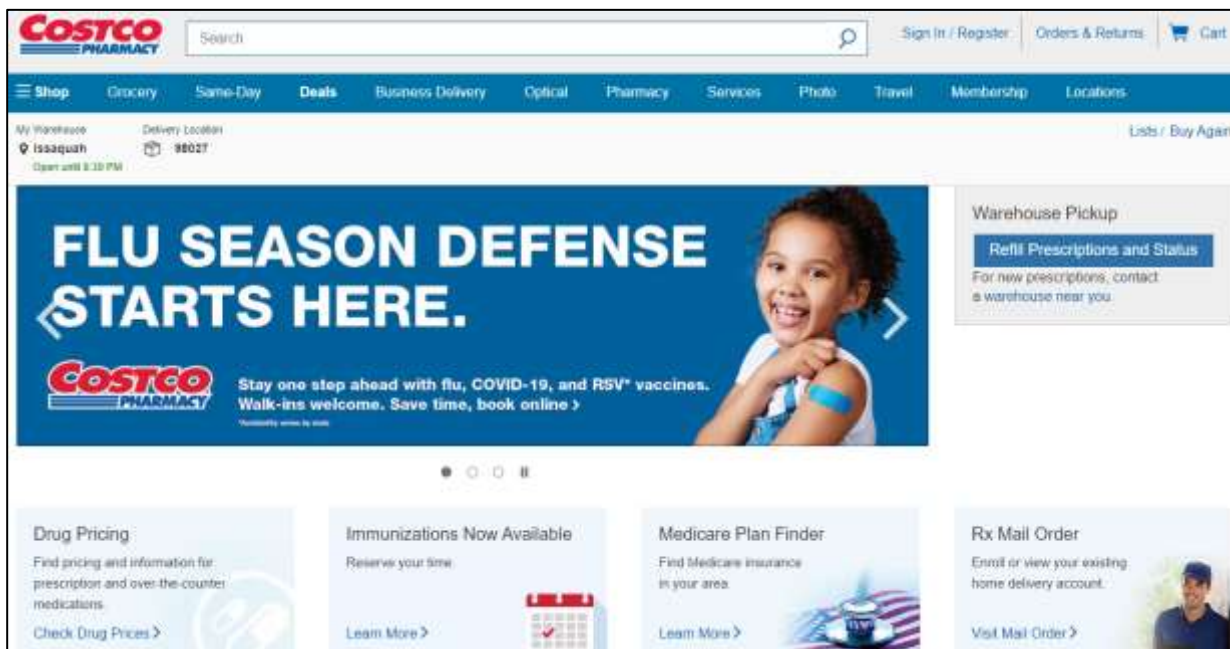
8 89. The Sensitive Information intercepted, recorded, and transmitted to Meta  
 9 includes, but is not limited to: patient status; prescription information (including specific drugs  
 10 and pricing information); immunization information; treatments; patient location; and health  
 11 insurance coverage. During that same transmission, Defendant would also provide Meta with  
 12 the patient's Facebook ID number, other persistent cookies, device ID, computer IP addresses,  
 13 or other PII. This information makes it easy to link private communications with Defendant via  
 14 the Website to a specific and identifiable Facebook user.

15 90. Once Meta has that data, it can process it, analyze it, and assimilate it into  
 16 databases like Core Audiences or Custom Audiences for advertising purposes. If the website  
 17 visitor is also a Facebook user, Meta will associate the information that it collects from the visitor  
 18 with a Facebook ID that identifies the user's name and Facebook profile. In sum, Pixel allows  
 19 Meta to learn, manipulate, and use for financial gain, the medical and private content Defendant's  
 20 Website visitors communicated, viewed, or otherwise interacted with on Defendant's Website.

#### 21 **D. Defendant Deployed Pixel to Intercept and Record Sensitive Information**

22 91. As an example of how Pixel operates on Defendant's Website, consider a visitor  
 23 who opens Defendant's Website, and navigates to the Pharmacy webpage. When doing so, the  
 24 visitor's browser sends a GET Request to Defendant's server, requesting that server to load the  
 25 Pharmacy webpage, which is displayed below in Figure 1:

26 <sup>47</sup>Meta Pixel, Facebook, [https://www.facebook.com/business/tools/meta-pixel?ref=search\\_new\\_2](https://www.facebook.com/business/tools/meta-pixel?ref=search_new_2) (last visited Sept. 14, 2023).



**Figure 1: Depiction of Pharmacy webpage**

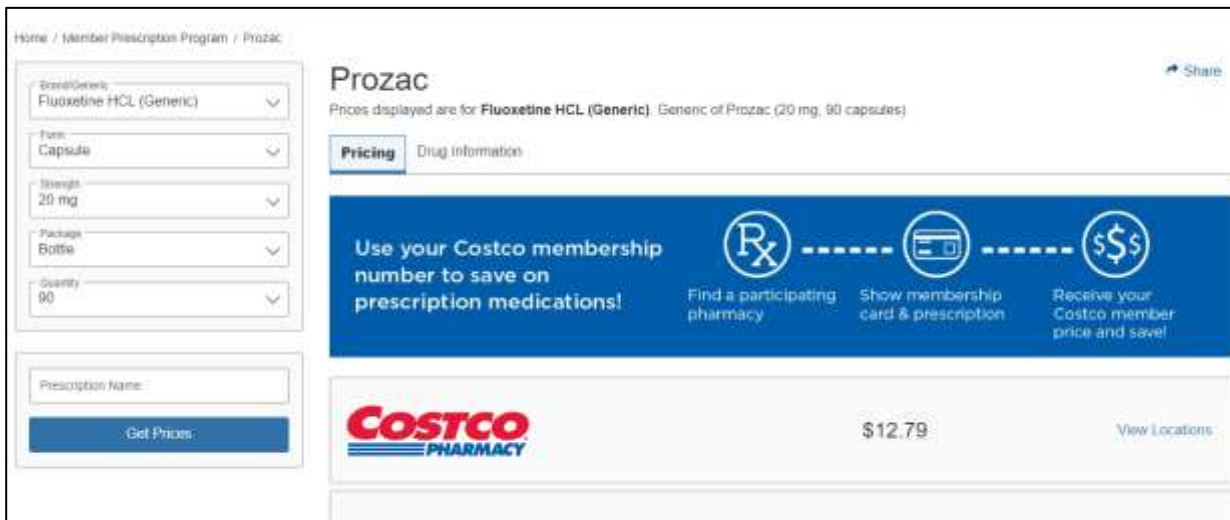
92. At the same time, Pixel causes the visitor's browser to intercept secretly and record the visitor's communication with Defendant's Website, including the specific URL requested, and transmit the private communication to Meta along with unique identifiers used to link the communication to a specific Facebook user, as shown in **Figure 2**:



**Figure 2: Depiction of information intercepted and recorded by Meta.**

93. As reflected in **Figure 2**, the “path” shows the specific URL for the page requested by the visitor’s browser. It also shows the Pixel’s transmission of the `_fbp` cookie, the `c_user` cookie (the Facebook ID), and other cookies and identifiers used to identify the website visitor by name and Facebook account. Thus, the fact that a Costco Pharmacy patient or prospective patient is using or considering using the Costco Pharmacy is transmitted to Meta. Disclosure of that information reveals to Meta the website visitor’s status as a patient or prospective patient with Costco Pharmacy.

94. If that same visitor to the Costco Pharmacy webpage navigates to the “Drug Pricing” subpage, and enters the name of a prescription medication in the search bar, such as “Prozac,”<sup>48</sup> the visitor’s browser communicates a GET request to Defendant’s server to load the page shown below in **Figure 3**:

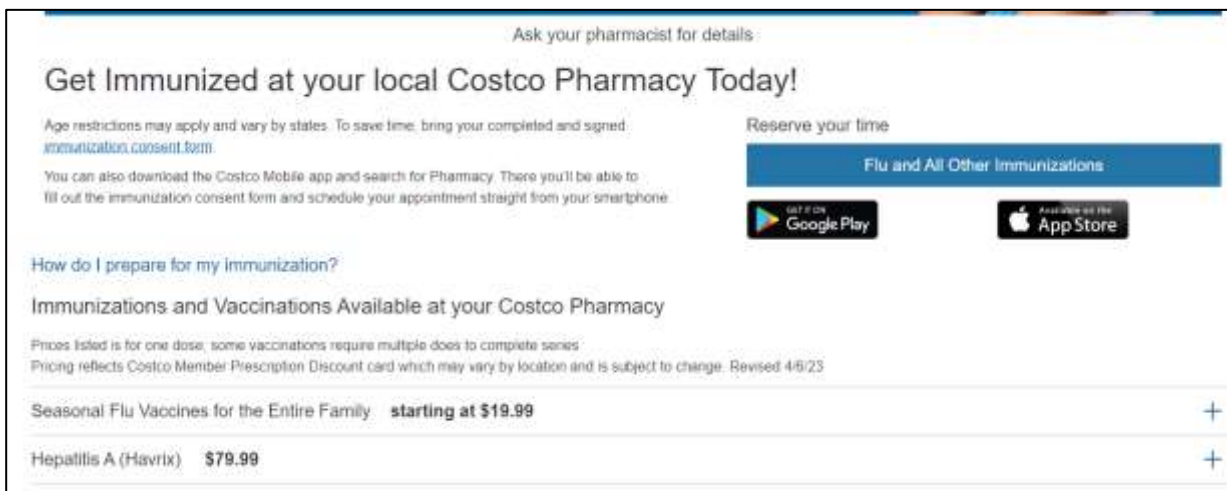


**Figure 3: Depiction of search for “Prozac” pricing**

95. Because Defendant’s Website uses Pixel, the visitor’s private communications to Defendant’s Website are also intercepted, recorded, and transmitted to Meta along with unique identifiers used to link the communications to a specific Facebook user, as shown in **Figure 4**:

<sup>48</sup> Prozac is a well-known antidepressant. Antidepressants, <https://my.clevelandclinic.org/health/treatments/9301-antidepressants-depression-medication> (last visited Sept. 19, 2023).

96. As another example, if a visitor to the Pharmacy webpage navigates to the “Immunizations Now Available,” subpage, the visitor can select from a variety of immunizations provided by Costco Pharmacy, including “Shingles (Shingrix),” resulting in the visitor’s browser transmitting a GET request to Defendant’s server to display the pages reflected below in ***Figures 5 and 6:***



**Figure 5: Depiction of “Immunizations Now Available” subpage.**

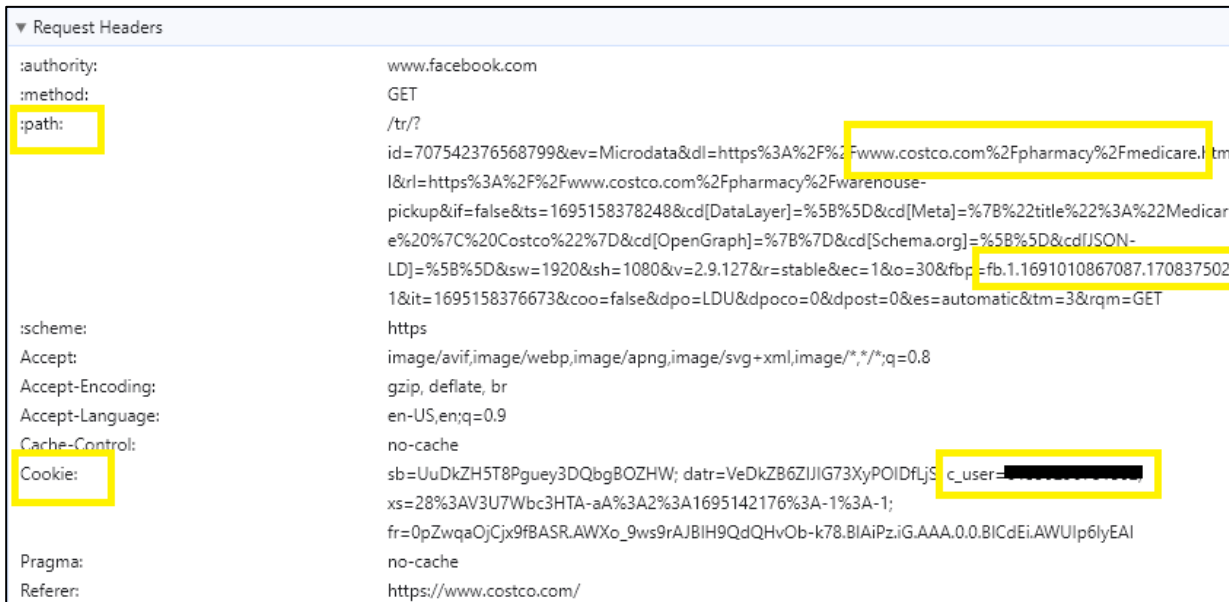


**Figure 6: Depiction of “Shingles” selection.**

97. Because Defendant’s Website uses Pixel, the visitor’s private communications to Defendant about a specific vaccine—Shingles (Shingrix)—are also intercepted, recorded, and transmitted to Meta along with unique identifiers used to link the communications to a specific Facebook user, as shown in **Figure 7**:

98. Similarly, if a visitor then navigates to the “Medicare Plan Finder” subpage within the Pharmacy webpage, the visitor’s browser communicates a GET request to Defendant’s server to display the page shown in **Figure 8**, and that private communication is also intercepted and recorded by Meta along with the visitor’s unique identifiers as shown in **Figure 9**:





**Figure 9: Depiction of “Medicare Plan Finder” intercepted and recorded by Meta.**

99. By intercepting this information, Meta would know, for example, that a particular Facebook user was in the market for Medicare Part D prescription drug plans. And Meta would be able to monetize that private information by selling advertising to insurance companies seeking to market their Medicare Part D coverage to seniors.

100. As a final example, if a visitor to the Costco Pharmacy webpage navigates to the “Rx Mail Order” subpage, and clicks on “Refill Prescription,” the visitor’s browser sends a GET request to Defendant’s server, which displays a “Sign In” page as shown in **Figure 10**, and the visitor’s private communication about refilling a prescription is intercepted and recorded by Meta along with unique identifiers as shown in **Figure 11**:

▼ Request Headers

:authority:	www.facebook.com
:method:	GET
:path:	/tr/?id=707542376568799&ev=SubscribedButtonClick&dl=https%3A%2F%2Fwww.costco.com%2Fpharmacy%2Fhome-delivery&l=https%3A%2F%2Fwww.costco.com%2Fpharmacy%2Fwarehouse-pickup&if=false&ts=1695160443103&cd[buttonFeatures]=%7B%22classList%22%3A%22btn%20btn-primary%20btn-block%22%2C%22destination%22%3A%22https%3A%2F%2Fwww.costco.com%2FPharmacy%2Fhome-delivery-refill-prescription%22%2C%22id%22%3A%22refill-prescription-button%22%2C%22imageUrl%22%3A%22%22%2C%22innerText%22%3A%22Refill%20Prescriptions%22%2C%22numChildButtons%22%3A0%2C%22tag%22%3A%22a%22%2C%22type%22%3Anull%2C%22name%22%3A%22%22%2D%2D&cd[buttonText]=Refill%20Prescriptions&cd[formFeatures]=%5B%5D&cd[pageFeatures]=%7B%22title%22%3A%22%22%20%20%20%20%20%20%20Costco%20Pharmacy%5Cn%20%20%20%20%20%22%2D%2D&sw=1920&sh=1080&v=2.9.127&r=stable&ec=2&o=10548&fbf=fb.1.1691010867087.1708375021&kcs_est=true&it=1695160398189&cco=false&dpo=LDU&dpoco=0&dpost=0&es=automatic&tms=3&rqm=GET
:scheme:	https
Accept:	image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Accept-Encoding:	gzip, deflate, br
Accept-Language:	en-US,en;q=0.9
Cache-Control:	no-cache
Cookie:	sb=UuDkZHST8Pguey3DQbgBOZHW; datr=VeDkZB6ZIIG73XyPOIDflj; c_user=[REDACTED]; s=28%3AV3U7Wbc3HTA-aA%3A2%3A1695142176%3A-1%3A-1; fr=0pZwqaOjCjx9FBASR.AWXo_gwsyrAJ8IH9QdQHvOb-k78.BIAiPz.iG.AAA.0.0.BICdEi.AWUIp6lyEI
Pragma:	no-cache
Referer:	https://www.costco.com/

101. Based on the above examples of how Pixel operates on the Costco Pharmacy webpage, Meta would know (1) that a particular individual—who Meta could identify by name from the individual’s Facebook account—was a patient or prospective patient of the Costco Pharmacy seeking healthcare services, (2) that the named patient searched for pricing information for Prozac, a well-known antidepressant medication, (3) that the named patient inquired about the Shingles vaccine, (4) that the named patient was trying to refill prescriptions; and (5) that the

1 named patient was in the market for Medicare Part D prescription coverage. Meta would also  
 2 know the named patient's location and IP address, among other identifiers associated with the  
 3 patient's computer or cell phone. Using this Sensitive Information, Meta could put the named  
 4 patient into a Core or Custom Audience for purposes of targeted advertising by Costco or any  
 5 other company seeking to advertise its services or products to individuals that fit the named  
 6 patient's profile.

7 102. In this way, Meta, Costco, and other third parties profit off Plaintiffs' and Class  
 8 Members' Sensitive Information without their knowledge, consent, or authorization.

9 103. Defendant deprived Plaintiffs and the Class Members of their privacy rights when  
 10 it: (a) embedded and implemented Pixel, which surreptitiously intercepted, recorded, and  
 11 disclosed Plaintiffs' and other online patients' and prospective patients' confidential  
 12 communications and private information; (b) disclosed patients' and prospective patients'  
 13 protected information to Meta—an unauthorized third party; and (c) failed to provide notice to  
 14 or obtain the consent from Plaintiffs and the Class Members to share their Sensitive Information  
 15 with others.

#### 16 **D. Exposure of Sensitive Information Creates a Substantial Risk of Harm**

17 104. The Federal Trade Commission ("FTC") has recognized that consumer data is a  
 18 lucrative (and valuable) form of currency. In an FTC roundtable presentation, former  
 19 Commissioner Pamela Jones Harbour underscored this point by reiterating that "most consumers  
 20 cannot begin to comprehend the types and amount of information collected by businesses, or why  
 21 their information may be commercially valuable. Data is currency."<sup>49</sup>

22 105. The FTC also issued, and regularly updates, guidelines for businesses to  
 23 implement reasonable data security practices and incorporate security into all areas of the  
 24 business. According to the FTC, reasonable data security protocols require, among other things:

25  
 26 <sup>49</sup> Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable,  
 at 2 (Dec. 7, 2009) [https://www.ftc.gov/sites/default/files/documents/public\\_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf](https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf) (last visited Sept. 13, 2023).

(1) using industry tested and accepted methods; (2) monitoring activity on networks to uncover unapproved activity; (3) verifying that privacy and security features function properly; and (4) testing for common vulnerabilities or unauthorized disclosures.<sup>50</sup>

106. The FTC cautions businesses that failure to protect Sensitive Information and the resulting privacy breaches can destroy consumers' finances, credit history, and reputations, and can take time, money, and patience to resolve the effect.<sup>51</sup> Indeed, the FTC treats the failure to implement reasonable and adequate data security measures as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

**E. Plaintiffs' and the Class's Sensitive Information is Valuable**

107. As many health care data industry experts have recognized, "[p]atients' medical data constitutes a cornerstone of the big data economy. A multi-billion dollar industry operates by collecting, merging, analyzing[,] and packaging patient data and selling it to the highest bidder."<sup>52</sup>

108. Thus, the personal, health, and financial information of Plaintiffs and the Class Members is valuable and has become a highly desirable commodity. Indeed, one of the world's most valuable resources is the exchange of personal data.<sup>53</sup>

109. Business News Daily reported that businesses collect personal data (i.e., gender, web browser cookies, IP addresses, and device IDs), engagement data (i.e., consumer interaction with a business's website, applications, and emails), behavioral data (i.e., customers' purchase histories and product usage information), and attitudinal data (i.e., consumer satisfaction data)

<sup>50</sup> *Start With Security, A Guide for Business*, FTC, <https://www.ftc.gov/business-guidance/resources/start-security-guide-business> (last visited Sept. 13, 2023).

<sup>51</sup> See *Taking Charge: What to Do if Your Identity is Stolen*, FTC, at 2 (2012), <https://www.myoccu.org/sites/default/files/pdf/taking-charge-1.pdf> (last visited Sept. 13, 2023).

<sup>52</sup> Niam Yaraghi, *Who should profit from the sale of patient data?*, The Brookings Institution (Nov. 19, 2018), <https://www.brookings.edu/blog/techtank/2018/11/19/who-should-profit-from-the-sale-of-patient-data/> (last visited Sept. 13, 2023).

<sup>53</sup> *The world's most valuable resource is no longer oil, but data*, THE ECONOMIST (May 6, 2017), <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> (last visited Sept. 13, 2023).

1 from consumers.<sup>54</sup> Companies then use this data to impact the customer experiences, modify their  
 2 marketing strategies, publicly disclose or sell data, and even to obtain more sensitive data that  
 3 may be even more lucrative.<sup>55</sup>

4 110. The power to capture and use customer data to manipulate products, solutions,  
 5 and the buying experience is invaluable to a business's success. Research shows that  
 6 organizations who "leverage customer behavioral insights outperform peers by 85 percent in  
 7 sales growth and more than 25 percent in gross margin."<sup>56</sup>

8 111. In 2013, the Organization for Economic Cooperation and Development  
 9 ("OECD") published a paper entitled "Exploring the Economics of Personal Data: A Survey of  
 10 Methodologies for Measuring Monetary Value."<sup>57</sup> In this paper, the OECD measured prices  
 11 demanded by companies concerning user data derived from "various online data warehouses."<sup>58</sup>

12 112. OECD indicated that "[a]t the time of writing, the following elements of personal  
 13 data were available for various prices: USD 0.50 cents for an address, USD 2 [i.e., \$2] for a date  
 14 of birth, USD 8 for a social security number (government ID number), USD 3 for a driver's  
 15 license number and USD 35 for a military record. A combination of address, date of birth, social  
 16 security number, credit record and military is estimated to cost USD 55."<sup>59</sup>

17 113. Unlike financial information, such as credit card and bank account numbers, the  
 18 PHI and certain PII cannot be easily changed. Dates of birth and social security numbers are  
 19  
 20  
 21

22 <sup>54</sup> Max Freedman, *How Businesses Are Collecting Data (And What They're Doing With It)*, BUSINESS NEWS DAILY  
 23 (Aug. 5, 2022; updated May 30, 2023), <https://www.businessnewsdaily.com/10625-businesses-collecting-data.html>  
 (last visited Sept. 13, 2023).

24 <sup>55</sup> *Id.*

25 <sup>56</sup> Brad Brown, et al. *Capturing value from your customer data*, MCKINSEY (Mar. 15, 2017),  
 26 [https://www.mckinsey.com/business-functions/quantumblack/our-insights/capturing-value-from-your-customer-](https://www.mckinsey.com/business-functions/quantumblack/our-insights/capturing-value-from-your-customer-data)  
 data (last visited Sept. 13, 2023).

<sup>57</sup> Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD  
 Digital Economy Papers, No. 220, OECD PUBLISHING PARIS (Apr. 2, 2013),  
<https://www.oecdilibrary.org/docserver/5k486qtxldmq-en.pdf> (last visited Sept. 13, 2023).

<sup>58</sup> *Id.* at 25.

<sup>59</sup> *Id.*

1 given at birth and attach to a person for the duration of his or her life. Medical histories are  
 2 inflexible. For these reasons, these types of information are the most lucrative and valuable.<sup>60</sup>

3 114. Consumers place considerable value on their Sensitive Information and the  
 4 privacy of that information. One 2002 study determined that U.S. consumers highly value a  
 5 website's protection against improper access to their Sensitive Information, between \$11.33 and  
 6 \$16.58 per website. The study further concluded that to U.S. consumers, the collective  
 7 "protection against errors, improper access, and secondary use of personal information is worth  
 8 between US\$30.49 and \$44.62.<sup>61</sup> This data is approximately twenty years old, and the dollar  
 9 amounts would likely be exponentially higher today.

10 115. Time Magazine published an article in 2017 titled "How Your Medical Data Fuels  
 11 a Hidden Multi-Billion Dollar Industry" in which it described the extensive market for health  
 12 data and observed that the market for information was both lucrative and a significant risk to  
 13 privacy.<sup>62</sup>

14 116. Similarly, CNBC published an article in 2019 in which it observed that "[d]e-  
 15 identified patient data has become its own small economy: There's a whole market of brokers  
 16 who compile the data from providers and other health-care organizations and sell it to buyers."<sup>63</sup>

17 117. Indeed, numerous marketing services and consultants offering advice to  
 18 companies on how to build their email and mobile phone lists—including those seeking to take  
 19 advantage of targeted marketing—direct putative advertisers to offer consumers something of  
 20  
 21  
 22

23 <sup>60</sup> *Calculating the Value of a Data Breach – What Are the Most Valuable Files to a Hacker?* Donnellon McCarthy  
 24 Enters (July 21, 2020), <https://www.dme.us.com/2020/07/21/calculating-the-value-of-a-data-breach-what-are-the-most-valuable-files-to-a-hacker/> (last visited Sept. 13, 2023).

25 <sup>61</sup> Il-Horn Hann, Kai-Lung Hui *et al.*, *The Value of Online Information Privacy: Evidence from the USA and*  
 26 *Singapore*, at 17, Marshall Sch. Bus., Univ. So. Cal. (Oct. 2002),  
<https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf> (last visited Sept. 13, 2023).

<sup>62</sup> See <https://time.com/4588104/medical-data-industry/> (last visited February 16, 2023).

<sup>63</sup> See <https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html> (last visited March 1, 2023).

1 value in exchange for their personal information. “No one is giving away their email address for  
2 free. Be prepared to offer a book, guide, webinar, course or something else valuable.”<sup>64</sup>

3 118. There is also a market for data in which consumers can participate. Personal  
4 information has been recognized by courts as extremely valuable. *See In re Marriott Int’l, Inc.,*  
5 *Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) (“Neither should the  
6 Court ignore what common sense compels it to acknowledge—the value that personal identifying  
7 information has in our increasingly digital economy. Many companies, like Marriott, collect  
8 personal information. Consumers too recognize the value of their personal information and offer  
9 it in exchange for goods and services.”).

10 119. Several companies have products through which they pay consumers for a license  
11 to track their data. Google, Nielsen, UpVoice, HoneyGain, and SavvyConnect are all companies  
12 that pay for browsing historical information.

13 120. Facebook also has paid users for their digital information, including browsing  
14 history. Until 2019, Facebook ran a “Facebook Research” app through which it paid \$20 a month  
15 for a license to collect browsing history information and other communications from consumers  
16 between the ages 13 and 35.

17 121. Additionally, healthcare data is extremely valuable to bad actors. Health care  
18 records may be valued at up to \$250 per record on the black market.<sup>65</sup>

19 122. Defendant’s privacy violations exposed a variety of Sensitive Information,  
20 including patient status, prescription information, immunization information, health insurance  
21 coverage, and other highly sensitive data.

22 123. PHI, like that exposed here, is likely even more valuable than Social Security  
23 numbers and just as capable of being misused.<sup>66</sup> PHI can be ten times more valuable than credit  
24

25 <sup>64</sup> VERO, HOW TO COLLECT EMAILS ADDRESSES ON TWITTER <https://www.getvero.com/resources/twitter-lead-generation-cards/>. (last visited Sep. 1, 2023).

26 <sup>65</sup> Tori Taylor, *Hackers, Breaches, and the Value of Healthcare Data*, *SecureLink* (June 30, 2021),  
<https://www.securelink.com/blog/healthcare-data-new-prize-hackers>.

<sup>66</sup> *FBI Cyber Division Bulletin: Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI (April 8, 2014), <https://publicintelligence.net/fbi-health-care-cyber-intrusions/#:~:text=>

card information.<sup>67</sup> This is because one's personal health history, including prior illness, surgeries, diagnoses, mental health, prescriptions, and the like cannot be changed or replaced, unlike credit card information and even, under difficult circumstances, Social Security numbers.<sup>68</sup>

124. Indeed, prescription records, blood tests, doctor notes, hospital visits, and insurance records are all sold to commercial companies, which gather years of health information on hundreds of millions of people and then sell it to other industries, like pharmaceutical companies who use the information to sell more drugs.<sup>69</sup> Some industry insiders and journalists are even calling hospitals the “brokers to technology companies” for their role in data sharing in the \$3 trillion healthcare sector.<sup>70</sup> “Rapid digitization of health records . . . have positioned hospitals as a primary arbiter of how much sensitive data is shared.”<sup>71</sup>

**F. Plaintiffs and the Class Had a Reasonable Expectation of Privacy in Their Interaction with Defendant's Website**

125. Consumers are concerned about companies, like Defendant, collecting their data and assume the data they provide, particularly highly sensitive medical and insurance data, will be kept secure and private.

126. In a recent survey related to Internet user expectations, most website visitors indicated that their detailed interactions with a website should only be used by the website and

(U)% 20Cyber% 20actors% 20will% 20likely, records% 20in% 20the% 20black% 20market. (last visited Sept. 13, 2023).

<sup>67</sup> Tim Greene, *Anthem hack: Personal data stolen sells for 10x Price of Stolen Credit Card Numbers*, <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last visited Sept. 13, 2023)).

<sup>68</sup> *Hackers Selling Healthcare Data in the Black Market*, INFOSEC (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/> (last visited Sept. 13, 2023). Social Security numbers are not easily replaced. In fact, to obtain a new number, a person must prove that he or she continues to be disadvantaged by the misuse—meaning an individual must prove actual damage has been done and will continue in the future. The Social Security Administration warns that the unauthorized disclosure of a Social Security number can lead to identity theft and fraud. Social Security Administration, *Identity Theft and Your Social Security Number*, at 1, 56, <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Sept. 13, 2023).

<sup>69</sup> Adam Tanner, *How Your Medical Data Fuels a Hidden Multi-Billion Industry*, TIME (Jan. 9, 2017), <https://time.com/4588104/medical-data-industry/> (last visited Sept. 13, 2023).

<sup>70</sup> Melanie Evans, *Hospitals Give Tech Giants Access to Detailed Medical Records*, THE WALL STREET JOURNAL (Jan. 20, 2020), <https://www.wsj.com/articles/hospitals-give-tech-giants-access-to-detailed-medical-records-11579516200> (last visited Sept. 13, 2023).

<sup>71</sup> *Id.*

1 not be shared with a party they know nothing about.<sup>72</sup> Thus, website visitors reasonably expect  
 2 that their interactions with a website should not be released to third parties unless explicitly  
 3 stated.<sup>73</sup>

4 127. The majority of Americans consider one of the most important privacy rights to  
 5 be the need for an individual's affirmative consent before a company collects and shares its'  
 6 customers' data.<sup>74</sup> A March 2000 BusinessWeek/Harris Poll found that 89 percent of respondents  
 7 were uncomfortable with web tracking schemes where data was combined with an individual's  
 8 identity.<sup>75</sup> The same poll found that 63 percent of respondents were uncomfortable with web  
 9 tracking even where the clickstream data was not linked to personally identifiable information.<sup>76</sup>  
 10 A July 2000 USA Weekend Poll showed that 65 percent of respondents thought that tracking  
 11 computer use was an invasion of privacy.<sup>77</sup>

12 128. Patients and website users act consistently with their expectation of privacy. For  
 13 example, following a new rollout of the iPhone operating software—which asks users for clear,  
 14 affirmative consent before allowing companies to track users—85 percent of worldwide users  
 15 and 94 percent of U.S. users chose not to allow such tracking.<sup>78</sup>

16 129. Like the greater population, Defendant's patients and prospective patients would  
 17 expect the highly sensitive medical information they provided to Defendant through the Website  
 18 to be kept secure and private.

---

20 <sup>72</sup> See *Privacy and Online Tracking Perceptions Survey Report* (March 2020), CUJOAI, at 15–19, Privacy  
 21 Survey\_03-24 (cujo.com) (indicating major concerns of survey respondents was illegal use of data and unethical  
 22 tracking and indicating respondents' belief that responsibility allocation falls on websites, and Internet users should  
 be able to turn to the websites themselves, for privacy breaches).

23 <sup>73</sup> Frances S. Grodzinsky, Keith W. Miller & Marty J. Wolf, *Session Replay Scripts: A Privacy Analysis*, THE  
 INFORMATION SOCIETY, 38:4, 257, 258 (2022).

24 <sup>74</sup> *Public Opinion on Privacy*, EPIC.ORG, <https://archive.epic.org/privacy/survey/>.

25 <sup>75</sup> *Id.*

26 <sup>76</sup> *Id.*

<sup>77</sup> *Id.*

<sup>78</sup> Margaret Taylor, *How Apple screwed Facebook*, WIRED (May 19, 2021), <https://www.wired.co.uk/article/apple-ios14-facebook>.

**G. Defendant's Conduct Violates HIPAA**

130. Under HIPAA, individuals' health information must be:

properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well-being. The [Privacy] Rule strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing.<sup>79</sup>

131. HIPAA "is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge."<sup>80</sup> The rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.<sup>81</sup>

132. HIPAA defines "protected health information" as "individually identifiable health information" that is "created or received by a health care provider" (or similar entities) that "[r]elates to past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual." 45 C.F.R. § 160.103. Identifiers such as patient-status (i.e., information that connects a particular user to a particular health care provider), medical conditions, prescription information, or health insurance coverage and payment, gathered in this case by the Tracking Tools through Costco's Website, constitute protected health information.

133. Additionally, HIPAA defines sensitive patient personal and health information as: (1) name; (2) home and work addresses; (3) home and work phone numbers; (4) personal and professional email addresses; (5) medical records; (6) prescriptions; (7) health insurance

<sup>79</sup> U.S. Dept. of Health & Human Services: Summary of the HIPAA Privacy Rule (Oct. 19, 2022), <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html> (last visited Aug. 27, 2023).

<sup>80</sup> *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*, Centers for Disease Control and Prevention (June 27, 2022), [https://www.cdc.gov/phlp/publications/topic/hipaa.html#:~:text=Health%20Insurance%20Portability%20and%20Accountability%20Act%20of%201996%20\(HIPAA\),-On%20This%20Page&text=The%20Health%20Insurance%20Portability%20and,the%20patient's%20consent%20or%20knowledge](https://www.cdc.gov/phlp/publications/topic/hipaa.html#:~:text=Health%20Insurance%20Portability%20and%20Accountability%20Act%20of%201996%20(HIPAA),-On%20This%20Page&text=The%20Health%20Insurance%20Portability%20and,the%20patient's%20consent%20or%20knowledge) (last visited Aug. 19, 2022).

<sup>81</sup> U.S. Dept. of Health & Human Services: Summary of the HIPAA Privacy Rule (Oct. 19, 2022), <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html> (last visited Aug. 28, 2023).

1 information; (8) billing information; (9) Social Security number; (10) spouse and children's  
 2 information; and/or (11) emergency contact information.<sup>82</sup>

3 134. To ensure protection of this private and sensitive information, HIPAA mandates  
 4 standards for handling PHI—the very data Defendant failed to protect. The privacy violations  
 5 described herein resulted from Defendant's failure to comply with several of these standards:

- 6 a. Violation of 45 C.F.R. § 164.306(a)(1): failing to ensure the confidentiality and  
 7 integrity of electronic protected health information that Defendant creates,  
 8 receives, maintains, and transmits;
- 9 b. Violation of 45 C.F.R. § 164.312(a)(1): Failing to implement technical policies  
 10 and procedures for electronic information systems that maintain electronic  
 11 protected health information to allow access only to those persons or software  
 12 programs that have been granted access rights;
- 13 c. Violation of 45 C.F.R. § 164.308(a)(1): Failing to implement policies and  
 14 procedures to prevent, detect, contain, and correct security violations;
- 15 d. Violation of 45 C.F.R. § 164.306(a)(2): Failing to protect against any reasonably  
 16 anticipated threats or hazards to the security or integrity of electronic protected  
 17 health information;
- 18 e. Violation of 45 C.F.R. § 164.306(a)(3): Failing to protect against any reasonably  
 19 anticipated uses or disclosures of electronic protected health information that  
 20 are not permitted or required under the privacy rules regarding individually  
 21 identifiable health information;
- 22 f. Violation of 45 C.F.R. § 164.306(a)(4): Failing to ensure compliance with HIPAA  
 23 security standard rules by its workforce;

26 <sup>82</sup> See *What is Considered Protected Health Information Under HIPAA*, HIPAA Journal (Jan. 2, 2022); U.S. Dept. of Health & Human Services: Summary of the HIPAA Privacy Rule, <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html> (last visited Aug. 28, 2023).

g. Violation of 45 C.F.R. § 164.502 et seq.: Impermissibly and improperly using and disclosing protected health information that is, and remains, accessible to unauthorized persons; and

h. Violation of 45 C.F.R. § 164.530(c): Failing to design, implement, and enforce policies and procedures establishing administrative, technical, and physical safeguards to reasonably protect the privacy of protected health information.

135. Additionally, according to the U.S. Department of Health and Human Services' Health Information Privacy Bulletin ("HHS Privacy Bulletin"), HIPAA covered entities cannot share PHI or PII to online tracking technology vendors for marketing purposes without first obtaining the individual's HIPAA-compliant authorization.<sup>83</sup> The HHS Privacy Bulletin explicitly states:

The HIPAA Rules apply when the information that regulated entities collect through tracking technologies or disclose to tracking technology vendors includes protected health information (PHI). Some regulated entities may share sensitive information with online tracking technology vendors and such sharing may be unauthorized disclosures of PHI with such vendors. **Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules.** For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.<sup>84</sup>

136. The HHS Privacy Bulletin also identifies several harms that may result from an impermissible disclosure of an individual's PHI, including:

identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI. Such disclosures can reveal incredibly sensitive information about an individual, including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment. While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that

<sup>83</sup> *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, U.S. DEPT. OF HEALTH AND HUMAN SERVICES (Dec. 1, 2022), <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html>.

<sup>84</sup> *Id.* (internal citations omitted) (emphasis in original).

1 they disclose PHI **only** as expressly permitted or required by the HIPAA Privacy Rule.<sup>85</sup>

2 137. According to HHS, HIPAA “[r]egulated entities disclose a variety of information  
3 to tracking technology vendors through tracking technologies placed on a regulated entity’s  
4 website or mobile app, including individually identifiable health information [] that the individual  
5 provides when they use regulated entities’ websites or mobile apps.”<sup>86</sup> The information an  
6 individual provides may include a “medical record number, home or email address, or dates of  
7 appointments, as well as an individual’s IP address or geographic location, medical device IDs,  
8 or any unique identifying code.”<sup>87</sup>

9 138. All of the above listed information that is collected on a regulated entity’s website,  
10 like Defendant’s Website, is PHI, “even if the individual does not have an existing relationship  
11 with the regulated entity and even if the [information], such as IP address or geographic location,  
12 does not include specific treatment or billing information like dates and types of health care  
13 services.”<sup>88</sup> When a regulated entity, again like Defendant, collects the individual’s information,  
14 that information connects the individual to the regulated entity (i.e., it is indicative that the  
15 individual has received or will receive health care services or benefits from the covered entity),  
16 and thus relates to the individual’s past, present, or future health or health care or payment for  
17 care.<sup>89</sup>

18 139. As a pharmacy and health care provider, delivering “services . . . related to the  
19 health of an individual,” including the “[s]ale or dispensing of a drug . . . in accordance with a  
20 prescription,” Defendant is a “covered entity” and therefore subject to the requirements under  
21 HIPAA.<sup>90</sup> See 45 C.F.R. § 160.103 (defining “covered entity,” “health care provider,” and “health  
22 care”). Yet, by embedding and deploying Pixel, Defendant blatantly disregarded these rules,  
23

24 <sup>85</sup> *Id.* (internal citations omitted) (emphasis in original).

25 <sup>86</sup> *Id.*

26 <sup>87</sup> *Id.*

<sup>88</sup> *Id.*

<sup>89</sup> *Id.*

<sup>90</sup> Defendant acknowledges as much given its Notice of Privacy Practices. *See supra*.

1 placing profit over patient privacy and confidentiality, and therein violated the rights of its  
2 patients and prospective patients.

### 3 **CLASS PERIOD**

4 140. For purposes of this Class Action Complaint, the Class Period corresponds to the  
5 period between October 2020 and the present and runs until such date as the Court enters an  
6 Order certifying any Count of this Class Action Complaint for class action treatment.

### 7 **CLASS ACTION ALLEGATIONS**

8 141. Plaintiffs bring this class action pursuant to Rule 23 of the Federal Rules of Civil  
9 Procedure on behalf of themselves and all others similar situated, as representatives of the  
10 following Classes:

#### 11 **Nationwide Class**

12 All individuals residing in the United States whose Sensitive Information was disclosed  
13 to a third party through Defendant's Website without authorization or consent during the  
14 Class Period.

#### 15 **California Subclass**

16 All individuals residing in California whose Sensitive Information was disclosed to a  
17 third party through Defendant's Website without authorization or consent during the  
18 Class Period.

#### 19 **Florida Subclass**

20 All individuals residing in Florida whose Sensitive Information was disclosed to a third  
21 party through Defendant's Website without authorization or consent during the Class  
22 Period.

23 142. Excluded from the Classes is Defendant; officers, directors, and employees of  
24 Defendant; any entity in which Defendant has a controlling interest in, is a parent or subsidiary  
25 of, or which is otherwise controlled by Defendant; and Defendant's affiliates, legal  
26 representatives, attorneys, heirs, predecessors, successors, and assignees. Also excluded are the  
Judges and Court personnel in this case and any members of their immediate families.

1 143. Plaintiffs reserve the right to modify and/or amend the Class definitions, as  
2 necessary.

3 144. All members of the proposed Classes are readily identifiable through Defendant's  
4 records.

5 145. All requirements for class certification under Fed. R. Civ. P. 23(a), 23(b)(2) and  
6 23(b)(3) are satisfied.

7 146. **Numerosity.** The members of the Classes are so numerous that joinder of all  
8 members of the Classes is impracticable. Plaintiffs are informed and believe that the proposed  
9 Classes include at least one million people. The precise number of the Class Members is unknown  
10 to the Plaintiffs but may be ascertained from Defendant's records.

11 147. **Commonality and Predominance.** This action involves common questions of  
12 law and fact to the Plaintiffs and the Class Members, which predominate over any questions only  
13 affecting individual Class Members. These common legal and factual questions include, without  
14 limitation:

- 15 a. Whether Plaintiffs' and Class Members' private communications were  
16 intercepted, recorded, and disclosed;
- 17 b. Whether the interception, recording, and disclosure of Plaintiffs' and Class  
18 Members' communications was consensual;
- 19 c. Whether Defendant owed Plaintiffs and the other Class Members a duty to  
20 adequately protect their Sensitive Information;
- 21 d. Whether Defendant owed Plaintiffs and the other Class Members a duty to secure  
22 their Sensitive Information from interception and disclosure via third-party  
23 tracking technologies;
- 24 e. Whether Defendant owed Plaintiffs and the other Class Members a duty to  
25 implement reasonable data privacy protection measures because Defendant  
26

accepted, stored, created, and maintained highly sensitive information concerning Plaintiffs and the Classes;

- f. Whether Defendant knew or should have known of the risk of disclosure of data through third-party tracking technologies;
- g. Whether Defendant breached its duty to protect the Sensitive Information of Plaintiffs and the other Class Members;
- h. Whether Defendant knew or should have known about the inadequacies of its privacy protection;
- i. Whether Defendant failed to use reasonable care and reasonable methods to safeguard and protect Plaintiffs' and the Classes' Sensitive Information from unauthorized disclosure;
- j. Whether proper data security measures, policies, procedures, and protocols were enacted within Defendant's computer systems to safeguard and protect Plaintiffs' and the Classes' Sensitive Information from unauthorized disclosure;
- k. Whether Defendant's conduct was the proximate cause of Plaintiffs' and the Classes' injuries;
- l. Whether Plaintiffs and the Class Members had a reasonable expectation of privacy in their Sensitive Information;
- m. Whether Plaintiffs and the Class Members suffered ascertainable and cognizable injuries as a result of Defendant's misconduct;
- n. Whether Plaintiffs and the Class Members are entitled to recover damages; and
- o. Whether Plaintiffs and the Class Members are entitled to other appropriate remedies including injunctive relief.

148. Defendant engaged in a common course of conduct giving rise to the claims asserted by Plaintiffs on behalf of themselves and the Classes. Individual questions, if any, are

1 slight by comparison in both quality and quantity to the common questions that control this  
2 action.

3 149. **Typicality.** Plaintiffs' claims are typical of those of other Class Members because  
4 Plaintiffs' Sensitive Information, like that of every other Class Member, was improperly  
5 disclosed by Defendant. Defendant's misconduct impacted all Class Members in a similar  
6 manner.

7 150. **Adequacy.** Plaintiffs will fairly and adequately represent and protect the interests  
8 of the members of the Classes and have retained counsel experienced in complex consumer class  
9 action litigation and intend to prosecute this action vigorously. Plaintiffs have no adverse or  
10 antagonistic interests to those of the Classes.

11 151. **Superiority.** A class action is superior to all other available methods for the fair  
12 and efficient adjudication of this controversy. The damages or other financial detriment suffered  
13 by individual Class Members are relatively small compared to the burden and expense that would  
14 be entailed by individual litigation of their claims against Defendant. The adjudication of this  
15 controversy through a class action will avoid the possibility of inconsistent and potentially  
16 conflicting adjudications of the asserted claims. There will be no difficulty in managing this  
17 action as a class action, and the disposition of the claims of the Class Members in a single action  
18 will provide substantial benefits to all parties and to the Court. Absent a class action, individual  
19 patients like Plaintiffs would find the cost of litigating their claims prohibitively high and would  
20 have no effective remedy for monetary relief.

21 152. Class Certification under Fed. R. Civ. P. 23(b)(2) is also appropriate. Defendant  
22 has acted or refused to act on grounds that apply generally to the Classes, thereby making  
23 monetary, injunctive, equitable, declaratory, or a combination of such relief appropriate. As  
24 Defendant continues to engage in the practices described herein, the risk of future harm to  
25 Plaintiffs and the Classes remains, making injunctive relief appropriate. The prosecution of  
26 separate actions by all affected individuals with injuries similar to Plaintiffs', even if possible,

1 would create a substantial risk of (a) inconsistent or varying adjudications with respect to  
 2 individual patients, which would establish potentially incompatible standards of conduct for  
 3 Defendant, and/or (b) adjudications with respect to individual patients which would, as a practical  
 4 matter, be dispositive of the interests of the other patients not parties to the adjudications, or  
 5 which would substantially impair or impede the ability to protect the interests of the Classes.  
 6 Further, the claims of individual patients in the defined Classes are not sufficiently large to  
 7 warrant vigorous individual prosecution considering all of the concomitant costs and expenses.

## 8 LEGAL CLAIMS

### 9 COUNT I

#### 10 **Violation of the Electronic Communications Privacy Act (“ECPA”)**

#### 11 **18 U.S.C. § 2511(1)**

#### 12 **(By Plaintiffs and on behalf of the Nationwide Class)**

13 153. Plaintiffs reallege and incorporate by reference every allegation contained in the  
 14 paragraphs above as though fully set forth herein.

15 154. The Electronic Communications Privacy Act (“ECPA”) protects against the  
 16 intentional interception, attempted interception, or the procurement of another person to intercept  
 17 or attempt to intercept any wire, oral, or electronic communication. *See* 18 U.S.C. § 2511(1)(a).

18 155. The ECPA further provides any person who:

19 (c) intentionally discloses, or endeavors to disclose, to any other person the contents of  
 20 any wire, oral, or electronic communication, knowing or having reason to know that the  
 21 information was obtained through the interception of a wire, oral, or electronic  
 22 communication in violation of this subsection;

23 (d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic  
 24 communication, knowing or having reason to know that the information was obtained  
 25 through the interception of a wire, oral, or electronic communication in violation of this  
 26 subsection.

Shall be punished as provided in subsection (4) or shall be subject to suit as provided in  
 subsection (5).

*Id.* §§ 2511(1)(c) & (d).

1           156. The primary purpose of the ECPA is to protect the privacy and security of  
2 communications as technology evolves.

3           157. Section 2520 provides a private right of action to any person whose wire or  
4 electronic communications are intercepted, disclosed, or intentionally used. Specifically, Section  
5 2520 states that “any person whose wire, oral, or electronic communication is intercepted,  
6 disclosed, or intentionally used in violation of [Chapter 119] may in a civil action recover from  
7 the person or entity . . . , which engaged in that violation” in a civil action. *Id.* § 2520(a).

8           158. Section 2520 provides for \$10,000 in statutory damages for violations of ECPA.  
9 *Id.* § 2520(c)(2)(B).

10           159. The ECPA defines “intercept[ion]” as the “acquisition of the contents of any wire,  
11 electronic, or oral communication through the use of any electronic, mechanical, or other device.”  
12 *Id.* § 2510(4).

13           160. The ECPA defines “contents,” when used with respect to electronic  
14 communications, to “include[] any information concerning the substance, purport, or meaning of  
15 that communication.” *Id.* § 2510(8).

16           161. “Electronic communication” means “any transfer of signs, signals, writing,  
17 images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio,  
18 electromagnetic, photoelectronic or photooptical system that affects interstate or foreign  
19 commerce.” *Id.* § 2510(12).

20           162. “Electronic, mechanical or other device” means “any device or apparatus which  
21 can be used to intercept . . . electronic communication[s].” *Id.* § 2510(5). Here, Plaintiffs’ and  
22 the Class Members’ browsers and computing devices and Defendant’s webserver, Website, and  
23 Pixel code and other tracking technologies Defendant deployed are all “devices” for the purposes  
24 of the ECPA.

25           163. The transmissions of PII and PHI from Plaintiffs and the Class Members to  
26 Defendant through Defendant’s Website (www.costco.com) are “electronic communications”

1 under the ECPA. *See id.* § 2510(12). The information transmitted by Plaintiffs and the Class  
 2 Members included, but was not limited to, information regarding patient status, past and current  
 3 prescription medications, treatments and care options, immunizations, location, medication  
 4 research, health insurance coverage, and other sensitive information.

5 164. Additionally, through its use of the Tracking Tools, Defendant intercepted and  
 6 disclosed the communications about patient status, prescriptions, underlying health conditions,  
 7 and other Sensitive Information Plaintiffs searched for on Defendant's Website. The  
 8 communications and information that Costco disclosed through third-party Tracking Tools  
 9 included detailed content, including prescriptions, underlying health conditions, and/or location  
 10 information, often transmitted together. This information was, in turn, used by third-parties, such  
 11 as Facebook, to 1) place Plaintiffs in specific health-related categories; and 2) target Plaintiffs  
 12 with particular advertising associated with Plaintiffs' particular health conditions. Defendant  
 13 knowingly transmitted this data and did so for the purpose of financial gain.

14 165. By embedding and deploying the Tracking Tools on Defendant's Website,  
 15 Defendant intentionally violated the ECPA, through its interception, attempt at interception, and  
 16 its procurement of third parties to intercept the electronic communications of Plaintiffs and the  
 17 Class Members. Defendant also intentionally used or attempted to use the contents of Plaintiffs'  
 18 and the Class Members' electronic communications, knowing that the information was obtained  
 19 through interception. Defendant's use of the intercepted information and data for its own  
 20 advertising and data analytics, in the absence of express written consent, violated ECPA.

21 166. Further, by embedding the Tracking Tools on its Website and disclosing the  
 22 content of patient communications relating to Sensitive Information, without consent, Defendant  
 23 had a purpose that was tortious, criminal, and designed to violate state and federal laws,  
 24 including:

- 25 a. An invasion of privacy;
- 26 b. A violation of the Washington Uniform Health Care Information Act;

- c. A violation of the Washington Consumer Protection Act;
- d. A violation of the Washington cybercrime act (RCW 9A.90);
- e. A violation of 42 U.S.C. § 1320d–6, the Administrative Simplification subtitle of HIPAA, which protects against the disclosure of individually identifiable health information to another person and is a criminal offense punishable by fine or imprisonment; and
- f. A violation of HIPAA.

167. Any party exception in 18 U.S.C. § 2511(2)(d) does not apply. The party exception in § 2511(2)(d) does not permit a party that intercepts or causes interception to escape liability if the communication is intercepted for the purpose of committing any tortious or criminal act in violation of the Constitution or laws of the United States or of any State. Here, as alleged above, Defendant violated a provision of the Health Insurance Portability and Accountability Act, specifically 42 U.S.C. § 1320d-6(a)(3).

168. 42 U.S.C. § 1320d-6(a)(3) provides criminal and civil penalties against a healthcare provider who “knowingly . . . discloses individually identifiable health information to another person.” Section 1320d(6) of HIPAA defines individually identifiable health information (“IIHI”) as:

any information, including demographic information collected from an individual, that—(A) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (B) *relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and—(i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.*

42 U.S.C. § 1320d(6) (emphasis added).

169. Guidance issued by HHS confirms that the Tracking Tools deployed by Defendant violates HIPAA. HIPAA prohibits disclosing patients’ health information via tracking technologies on both user-authenticated webpages (such as the log-in portal) and unauthenticated webpages. The guidance includes in the definition of IIHI the types of information intercepted

1 by the Tracking Tools on Defendant's Website, including information that "relates to the past,  
 2 present, or future physical or mental health or condition of an individual," such as prescription  
 3 information. Defendant's use of the Tracking Tools violates HIPAA because the Meta Pixel and  
 4 the other Tracking Tools also transmit information that "identifies the individual" or, at a  
 5 minimum, "there is a reasonable basis to believe that the information can be used to identify the  
 6 individual," such as through unique identifying cookies and users' IP addresses. As described  
 7 above, Plaintiffs entered data on Defendant's Website relating to prescriptions and other  
 8 Sensitive Information, and some later received advertisements from Costco. This shows that  
 9 through the Tracking Tools employed, Defendant disclosed the individually identifiable health  
 10 information of its Website visitors to third parties in violation of the ECPA.

11 170. At no time did Plaintiffs and the Class Members provide their consent to  
 12 Defendant's disclosure of their Sensitive Information to Meta and/or other third parties. Plaintiffs  
 13 and the Class had a reasonable expectation that Defendant would not re-direct their  
 14 communications content to Meta, Google, or others attached to their personal identifiers in the  
 15 absence of their knowledge or consent.

16 171. Further, Defendant has improperly profited from its invasion of Plaintiffs' and the  
 17 Class Members' privacy in its use of their data for its economic value.

18 172. Defendant knew that such conduct would be highly offensive. Regardless, it  
 19 proceeded to embed the Tracking Tools and use them to the detriment of visitors to its Website.

20 173. Plaintiffs and the Class Members are entitled to damages, including statutory,  
 21 compensatory and/or nominal damages in an amount to be proven at trial.

22 174. Defendant's conduct is ongoing, and it continues to unlawfully disclose and use  
 23 the intercepted communications of Plaintiffs and the Class Members any time they provide  
 24 information to Defendant through its Website without their consent. Plaintiffs and the Class  
 25 Members are therefore entitled to declaratory and injunctive relief. Such relief will prevent future  
 26

1 unlawful and unauthorized disclosure of Plaintiffs' and the Class Members' Sensitive  
2 Information.

### 3 **COUNT II**

#### 4 **Violation of the Washington Privacy Act**

5 **Wash. Rev. Code § 9.73.030 et seq.**

6 **(By Plaintiffs and on behalf of the Nationwide Class)**

7 175. Plaintiffs reallege and incorporate by reference every allegation contained in the  
8 paragraphs above as though fully set forth herein.

9 176. The Washington Privacy Act (the "Act") makes it unlawful for "any individual,  
10 partnership, corporation, [or] association . . . to intercept[] or record" any "[p]rivate  
11 communication transmitted by telephone, telegraph, radio, or other device between two or more  
12 individuals between points within or without the state by any device electronic or otherwise  
13 designed to record and/or transmit said communication regardless how such device is powered  
14 or actuated, without first obtaining the consent of all the participants in the communication."  
15 Wash. Rev. Code § 9.73.030(1)(a).

16 177. The Act further states that "[a]ny person who, directly or by means of a detective  
17 agency or any other agent, violates the provisions of [Chapter 9.73] shall be subject to legal action  
18 for damages, to be brought by any other person claiming that a violation of this statute has injured  
19 his or her business, his or her person, or his or her reputation. A person so injured shall be entitled  
20 to actual damages, including mental pain and suffering endured by him or her on account of  
21 violation of the provisions of [Chapter 9.73], or liquidated damages computed at the rate of one  
22 hundred dollars a day for each day of violation, not to exceed one thousand dollars, and a  
reasonable attorney's fee and other costs of litigation." *Id.* § 9.73.060.

23 178. Costco is a person for purposes of the Act because it is a corporation. *Id.* §§  
24 9.73.030(1), 9.73.060.

25 179. Plaintiffs' and the Class Members' intercepted and recorded Website  
26 Communications related to their Sensitive Information constitute "private communications"  
within the meaning of the Act. *See id.*

1 180. Plaintiffs' and the Class Members' electronic devices and web browsers, and  
2 Defendant's webserver and Website are "devices" through which the private communications  
3 were transmitted between points within or without the state of Washington.

4 181. Online tracking technology like Pixel, provided by Meta and procured by  
5 Defendant, is a "device" that is "designed to record and/or transmit [private] communications"  
6 within the meaning of the Act. *See id.* § 9.73.030(1)(a).

7 182. Defendant intentionally procured and embedded the Tracking Tools on its  
8 Website, including on its Pharmacy webpage, to secretly intercept and record Plaintiffs' and the  
9 Class Members' private communications with Costco in real time, including communications  
10 regarding prescriptions and immunizations, among other Sensitive Information. Defendant  
11 violated the Act directly and by means of agents by intercepting and recording Plaintiffs' and  
12 Class Members' private communications with Defendant via the Tracking Tools.

13 183. Defendant did so for its own profit and gain, disclosing its patients' and  
14 prospective patients' sensitive health information to third parties, like Meta, in an effort to drive  
15 visits to its website using more sophisticated and targeted advertising based on data harvested  
16 from its website visitors.

17 184. As participants in the communications, Plaintiffs and the Class Members did not  
18 consent to having their Website Communications secretly intercepted and recorded.

19 185. As a direct and proximate result of Defendant's conduct, Plaintiffs and the Class  
20 Members were injured in their "person[s]," RCW 9.73.060, including through interference with  
21 their control over their personal data, intrusion into their private affairs, the highly offensive  
22 publication of private facts, and other losses of privacy related to the secret interception and  
23 disclosure of their private and sensitive health information.

24 186. Under Section 9.73.060, Plaintiffs and the Class Members seek (1) actual  
25 damages, not less than liquidated damages computed at the rate of one hundred dollars a day for  
26

each day of violation, not to exceed one thousand dollars, and (2) reasonable attorneys' fees and other costs of litigation incurred. Wash. Rev. Code § 9.73.060.

### **COUNT III**

#### **Violation of the Washington Consumer Protection Act ("WCPA") Wash. Rev. Code § 19.86 et seq. (By Plaintiffs and on behalf of the Nationwide Class)**

187. Plaintiffs reallege and incorporate by reference every allegation contained in the paragraphs above as though fully set forth herein.

188. The Washington Consumer Protection Act ("WCPA"), Washington Revised Code Section 19.86 et seq., prohibits "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce." Wash. Rev. Code § 19.86.020.

189. The elements of a WCPA claim are (1) an unfair or deceptive act or practice, (2) occurring in trade or commerce, (3) impacting the public interest, (4) an injury to plaintiff in her business or property, and (5) a causal relationship between the unfair or deceptive act and the resulting injury. *Hangman Ridge Training Stables, Inc. v. Safeco Title Ins. Co.*, 719 P.2d 531, 535–40 (Wash. 1986).

190. Defendant engaged in unfair or deceptive acts, omissions, and practices in the conduct of trade or commerce, in violation of Section 19.86.020, by violating Plaintiffs' and the Class Members' rights to privacy and by embedding and implementing Tracking Tools, like Pixel, on its Website, to secretly record and disclose Plaintiffs' and the Class Members' private communications, including their highly sensitive health information, without their consent.

191. Defendant shared its collected data with third parties, like Meta, for profit or other business purposes, which further violates the WCPA and is an unfair or deceptive act or practice.

192. Defendant committed its conduct in the context of trade or commerce. Costco offers pharmaceutical services and other health-related services in interstate commerce in markets across the nation. In addition, visitors to Costco's Website can use the Website to purchase prescriptions, immunizations, and conduct other health-related activities. Costco uses its covert interception of patients' and prospective patients' Website Communications, including

1 Sensitive Information, for business purposes affecting interstate commerce, including by  
 2 providing patient and prospective patient personal and health-related data to third parties for  
 3 profit.

4 193. The public interest is harmed by Defendant's conduct in embedding and  
 5 implementing the Tracking Tools on its Website to intercept, record, and disclose millions of  
 6 Americans' private and protected communications, including their highly personal information,  
 7 to unauthorized third parties. This includes Plaintiffs and the Class Members who have a  
 8 fundamental privacy interest in that information. Indeed, Costco's unlawful procurement of  
 9 individuals' personal and health-related data, some of the most sensitive nature, without their  
 10 consent has large ramifications on the privacy interest of those individuals. In addition, to the  
 11 extent that Costco uses this information for improvements to its services or transmits such  
 12 information to third parties for profit or another benefit, Costco is deriving an unfair competitive  
 13 advantage because of its covert recording and unauthorized disclosures.

14 194. Plaintiffs' and the Class Members' property has been harmed by Defendant's  
 15 unfair and deceptive practices. Plaintiffs' and the Class Members' PII and PHI is inherently  
 16 valuable. Plaintiffs and the Class Members have been deprived of the value inherent in their  
 17 personal information that Defendant unlawfully disclosed to third parties. A market exists for the  
 18 collection of patient data, including an individual's personal, health, and financial information,  
 19 and companies will—and must—pay a premium to obtain this valuable commodity. Accordingly,  
 20 Plaintiffs and the Class Members have a property interest in their private information and thus  
 21 were deprived of appropriate consideration and compensation for the unauthorized data-sharing  
 22 with third parties of Plaintiffs' and the Class Members' private and protected communications  
 23 without consent or consideration.

24 195. Plaintiffs and the Class Members have been harmed in their privacy interests by  
 25 Defendant's embedding of the Tracking Tools on its Website and disclosing, without consent,  
 26 the content of patient and prospective patient communications relating to prescriptions and

1 immunizations, among other Sensitive Information. Furthermore, Defendant's actions have and  
 2 continue to injure Plaintiffs and the Class Members because their private communications,  
 3 including their highly sensitive health information, is being used, and continues to be used, for  
 4 commercial gain—all without their knowledge or consent.

5 196. Plaintiffs and the Class Members expected their communications would remain  
 6 private such that they could freely interact with Defendant's Website and disclose private,  
 7 personal information for the purpose of receiving health care services or health care-related  
 8 information and knowledge. At no time did Plaintiffs and the Class Members ever expect that  
 9 Costco would unlawfully and surreptitiously share their private and protected communications,  
 10 including their highly personal health information, to third parties by using embedded third-party  
 11 tracking technologies, like Pixel, on Defendant's Website. Such considerations are material to  
 12 Plaintiffs and the Class Members as reasonable consumers. Had Plaintiffs and the Class Members  
 13 known of Costco's unlawful conduct, they would not have interacted with its Website, including,  
 14 for example, by purchasing prescriptions through its Website, nor relied on its health care  
 15 services, or they would have demanded compensation for such data sharing.

16 197. Defendant's conduct is unfair as it offends public policy as established by statute  
 17 and is otherwise unethical, oppressive, or unscrupulous.

18 198. These unfair and deceptive acts are the proximate cause of the alleged injuries.

19 199. Plaintiffs and the Class Members are entitled to damages, statutory treble  
 20 damages, and reasonable attorneys' fees under Washington Revised Code Section 19.86.090.

#### 21 **COUNT IV**

#### 22 **Violation of the Washington Uniform Health Care Information Act ("UHCIA")**

23 **Wash. Rev. Code. § 70.02 et seq.**

24 **(By Plaintiffs and on behalf of the Nationwide Class)**

25 200. Plaintiffs reallege and incorporate by reference every allegation contained in the  
 26 paragraphs above as though fully set forth herein.

201. The Washington Uniform Health Care Information Act ("UHCIA") defines a  
 "health care provider" as "a person who is licensed, certified, registered, or otherwise authorized

1 by the law of this state to provide health care in the ordinary course of business or practice of a  
 2 profession.” Wash. Rev. Code § 70.02.010(19).

3 202. The UHCIA defines “health care” as “any care, service, or procedure provided by  
 4 a health care provider,” including “[t]o diagnose, treat, or maintain a patient’s physical or mental  
 5 condition; or [t]hat affects the structure or any function of the human body.” *Id.* § 70.02.010(15).

6 203. Costco is a “health care provider” under the UHCIA because it is authorized to  
 7 provide health care services, including pharmaceutical services, and it provides care and services  
 8 that treat a patient’s physical or mental condition and that affects the structure or functions of the  
 9 human body, including, for example, the sale and dispensing of prescription drugs used in the  
 10 treatment of a patient’s physical or mental health or medical condition.

11 204. Plaintiffs and the Class Members are “patients” at all relevant times as that term  
 12 is defined under the UHCIA because they are “individual[s] who receive[] or ha[ve] received  
 13 health care.” *Id.* § 70.02.010(34).

14 205. In addition, the UHCIA defines “health care information” as “any information,  
 15 whether oral or recorded in any form or medium, that identifies or can readily be associated with  
 16 the identity of a patient and directly relates to the patient’s health care” and “includes any required  
 17 accounting of disclosures of health care information.” *Id.* § 70.02.010(17).

18 206. The information Plaintiffs and the Class Members communicated with Defendant  
 19 on its Website concerned the past, present, and future physical or mental health or condition and  
 20 the provision of health care. This information directly relates to a patient’s health care and can  
 21 be identified, or can be readily associated with the identity of, a patient. Thus, that information  
 22 constitutes “health care information” as that term is defined in the UHCIA.

23 207. Under the UHCIA, it is unlawful for a third party to access a patient’s health care  
 24 records from a provider, or a person who receives records from a provider, without the patient or  
 25 the patient’s legally authorized representative’s consent, specific authorization in law, or a  
 26

1 representative from a provider that holds a signed and dated consent from the patient authorizing  
2 the release. *Id.* §§ 70.02.020(1), 70.02.030(1), (3)–(4).

3 208. Under the UHCIA, it is unlawful for a health care provider, its agents, employees,  
4 and those who assist a health care provider in the delivery of health care to “disclose health care  
5 information about a patient to any other person without the patient’s written authorization.” *Id.* §  
6 70.02.020(1).

7 209. The UHCIA further prohibits a health care provider to “use or disclose health care  
8 information for marketing” or “[s]ell health care information to a third party” without the  
9 patient’s authorization. *Id.* §§ 70.02.280(1) & (2)(h).

10 210. Defendant’s use of the Tracking Tools resulted in Defendant disclosing to a third  
11 parties Plaintiffs’ and the Class Members’ health care information and, furthermore, allowed a  
12 third parties to access, without authorization, Plaintiffs’ and the Class Members’ health care  
13 information.

14 211. Neither Plaintiffs nor the Class Members consented to or otherwise authorized  
15 Defendant to share their private health care information with Meta or any other third party. Under  
16 the UHCIA, a health care provider or other person who causes an unauthorized release of health  
17 care information by disclosing such information in violation of the UHCIA shall be subject to  
18 suit and may be liable to the patient for compensatory damages, plus costs and reasonable  
19 attorneys’ fees. *Id.* § 70.02.170(1)–(2). As a result of Defendant’s violations of the UHCIA,  
20 Plaintiffs and the Class Members seek all damages authorized by law, including compensatory  
21 damages, plus costs and reasonable attorneys’ fees.

## 22 COUNT V

### 23 **Violation of the California Invasion of Privacy Act (“CIPA”)** 24 **Cal. Penal Code § 630, et seq** **(By Plaintiffs and on behalf of the California Class)**

25 212. Plaintiffs reallege and incorporate by reference every allegation contained in the  
26 paragraphs above as though fully set forth herein.

1           213. The California Invasion of Privacy Act (“CIPA”) is codified at Cal. Penal Code  
2 §§ 630 to 638. The Act begins with its statement of purpose.

3           The Legislature hereby declares that advances in science and technology have led  
4 to the development of new devices and techniques for the purpose of eavesdropping  
5 upon private communications and that the invasion of privacy resulting from the  
6 continual and increasing use of such devices and techniques has created a serious  
7 threat to the free exercise of personal liberties and cannot be tolerated in a free and  
8 civilized society.

9 Cal. Penal Code § 630.

10           214. California Penal Code § 631(a) provides, in pertinent part (emphasis added):

11           Any person who, by means of any machine, instrument, or contrivance, or in any  
12 other manner ... willfully and without the consent of all parties to the  
13 communication, or in any unauthorized manner, reads, or attempts to read, or to  
14 learn the contents or meaning of any message, report, or communication while the  
15 same is in transit or passing over any wire, line, or cable, or is being sent from, or  
16 received at any place within this state; or who uses, or attempts to use, in any  
17 manner, or for any purpose, or to communicate in any way, any information so  
18 obtained, or **who aids, agrees with, employs, or conspires** with any person or  
19 persons to unlawfully do, or permit, or cause to be done any of the acts or things  
20 mentioned above in this section, is punishable by a fine not exceeding two thousand  
21 five hundred dollars (\$2,500).

22           215. Under CIPA, a defendant must show it had the consent of all parties to a  
23 communication.

24           216. At all relevant times, Defendant aided, employed, agreed with, and conspired with  
25 unauthorized third parties to track and intercept Plaintiffs’ and Class Members’ communications  
26 made via the Website. These communications were transmitted to and intercepted by a third party  
during the communications and without the knowledge, authorization, or consent of Plaintiff and  
Class Members.

          217. Defendant intentionally inserted an electronic listening device onto Plaintiffs’ and  
Class Members’ web browsers that, without the knowledge and consent of Plaintiffs and Class  
Members, tracked and transmitted the substance of their confidential communications with  
Defendant to a third party.

218. Defendant willingly facilitated third parties' interception and collection of Plaintiffs' and Class Members' private medical information by embedding the Meta Pixel and other tracking technologies on its Website. Moreover, unlike past Facebook business tools such as the Facebook Like Button and older web beacons, Defendant has full control over the Pixel, including which webpages contain the pixel, what information is tracked and transmitted via the Pixel, and how events are categorized prior to their transmission.

219. The Meta Pixel and other Tracking Tools constitute a "machine, instrument, or contrivance" under the CIPA, and even if they do not, they fall under the broad catch-all category of "any other manner."

220. Defendant failed to disclose its use of the Pixel and other tracking technologies to specifically track and automatically and simultaneously transmit Plaintiffs' and Class Members' communications with Defendant to undisclosed third parties.

221. The Sensitive Information that Defendant transmitted via the Pixel, such as specific prescriptions, as well as names, IP addresses, home addresses, FIDs, or other identifying information, constitutes information about Plaintiffs' and Class Members' past, present, or future health or health care and therefore constitutes protected health information.

222. The Pixel is designed such that it transmits each of the actions users take on the Website to a third party alongside and contemporaneously with the user initiating the communication. Thus, the communication is intercepted in transit to the intended recipient, Defendant, and before it reaches Defendant's server.

223. As demonstrated above, Defendant violated CIPA by aiding and permitting third parties to intercept and receive its patients' online communications in real time through its Website. These interceptions occurred without Plaintiffs' and Class Members' consent, and unauthorized third parties (including, but not limited to, Meta) would not have received the contents of these communications but for Defendant's actions and use of the Tracking Tools.

224. By disclosing Plaintiffs' and Class Members' Sensitive Information, Defendant violated Plaintiffs' and Class Members' statutorily protected right to privacy.

225. As a result of the above violations and pursuant to CIPA Section 637.2, Defendant is liable to Plaintiffs and Class Members for treble actual damages related to their loss of privacy in an amount to be determined at trial or for statutory damages in the amount of \$5,000 per violation. Section 637.2 specifically states that "[it] is not a necessary prerequisite to an action pursuant to this section that the plaintiffs has suffered, or be threatened with, actual damages."

226. Under the statute, Defendant also is liable for reasonable attorneys' fees, litigation costs, and injunctive and declaratory relief.

**COUNT VI**  
**Violation of the California Confidentiality of Medical Information Act ("CMIA")**  
**Cal. Civ. Code § 56, et seq**  
**(By Plaintiffs and on behalf of the California Class)**

227. Plaintiffs reallege and incorporate by reference every allegation contained in the paragraphs above as though fully set forth herein.

228. The California Confidentiality of Medical Information Act, Cal. Civ. Code § 56, et seq ("CMIA") prohibits health care providers from disclosing medical information relating to their patients without a patient's authorization. Medical information refers to "any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care... regarding a patient's medical history, mental or physical condition, or treatment." "Individually Identifiable" means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual..." Cal. Civ. Code § 56.05.

229. Defendant is a healthcare provider as defined by Cal. Civ. Code § 56.06.

230. Plaintiffs and Class Members are patients of Defendant and, as a health care provider, Defendant has an ongoing obligation to comply with the CMIA's requirements with respect to Plaintiff's and Class Members' confidential medical information.

231. As set forth above, names, addresses, telephone numbers, email addresses, device identifiers, web URLs, IP addresses, and/or other characteristics that can uniquely identify specific patients are transmitted to unauthorized third parties in combination with patient prescription drug information and queries. This protected health information and personally identifiable information constitutes confidential information under the CMIA.

232. Pursuant to the CMIA, the information communicated to Defendant and disclosed to third parties constitutes medical information because it is patient information derived from a health care provider regarding patients' medical treatment and physical condition and is received by third parties in combination with individually identifying information. Cal. Civ. Code § 56.05(i).

233. As set forth above, Facebook views, processes, and analyzes the confidential medical information it receives via the Meta Pixel. It then uses the viewed confidential information to create Audiences for advertising and marketing purposes.

234. Defendant failed to obtain Plaintiffs' and Class Members' authorization for their disclosure of medical information.

235. Pursuant to CMIA Section 56.11, a valid authorization for disclosure of medical information must: (1) be "clearly separate from any other language present on the same page and ... executed by a signature which serves no other purpose than to execute the authorization;" (2) be signed and dated by the patient or their representative; (3) state the name and function of the third party that receives the information; and (4) state a specific date after which the authorization expires. The information set forth on Defendant's Website, including the Website Privacy Policy and Notice of Privacy Practices, does not qualify as a valid authorization.

236. Defendant thus violated the CMIA by disclosing its patients' medical information to third parties along with the patients' individually identifying information.

237. Plaintiff and Class Members seek nominal damages, compensatory damages, attorneys' fees, and costs of litigation for Defendant's violations of the CMIA.

**COUNT VII**

**Violation of the Florida Security of Communications Act**

**Fla. Stat. § 934.10(1), *et seq.***

**(By Plaintiff Washington and on behalf of the Florida Class)**

238. Plaintiff Washington realleges and incorporates by reference every allegation contained in the paragraphs above as though fully set forth herein.

239. The Florida Security of Communications Act (“FSCA”) is codified at Florida Statutes, § 934.01, *et seq.* The FSCA begins with legislative findings, including:

On the basis of its own investigations and of published studies, the Legislature makes the following findings...(4) to safeguard the privacy of innocent persons, the interception of wire or oral communications when none of the parties to the communications has consented to the interceptions should be allowed only when authorized by a court of competent jurisdiction and should remain under the control and supervision of the authorizing court.

240. Florida Statutes § 934.10 provides, in pertinent part, as follows:

Any person whose wire, oral, or electronic communication is intercepted, disclosed, or used in violation of §§ 934.04-934.09 shall have a civil cause of action against any person or entity who intercepts, discloses, or uses, or procures any person or entity to intercept, disclose, or use, such communications and shall be entitled to recover from any such person or entity which engaged in that violation such relief as may be appropriate, including: (a) [p]reliminary or equitable declaratory relief as may be appropriate; (b) [a]ctual damages, but not less than liquidated damages computed at the rate of \$100 a day for each day of the violation or \$1,0000, whichever is higher; (c) [p]unitive damages; and (d) [a] reasonable attorney’s fee and other litigation costs reasonably incurred.

241. The FSCA defines “electronic communication” as “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo-optical systems that affects intrastate, interstate, or foreign commerce.” Fla. Stat. § 934.02(12). It further defines “intercept” as “the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.” Fla. Stat. § 934.02(3).

1           242. At all relevant times, Defendant aided, employed, agreed with, and conspired with  
 2 Meta and other third parties to intercept Plaintiff's and Class Members' internet communications  
 3 while accessing the Website, including the contents thereof—*i.e.*, the URL visited, the  
 4 prescriptions searched for or ordered, and the associated underlying health conditions. Such  
 5 information not only constitutes protected health information, it also represents the substance,  
 6 import, and meaning of the communications between Plaintiff and other Class Members had with  
 7 Defendant's Website.

8           243. Plaintiff and other Class Members had a reasonable expectation of privacy in the  
 9 electronic communications they had with Defendant's Website.

10           244. Nonetheless, these electronic communications were transmitted to and intercepted  
 11 by third parties, including Meta, during the communication and without knowledge,  
 12 authorization, or consent of Plaintiff and Class Members. That is because Defendant intentionally  
 13 inserted an electronic device into its website that, without the knowledge and consent of Plaintiff  
 14 and Class Members, recorded and transmitted the substance of their confidential communications  
 15 with Defendant to third parties.

16           245. Defendant willingly facilitated third parties' interception and collection of  
 17 Plaintiff's and Class Members' Sensitive Information by embedding the Tracking Tools on its  
 18 Website.

19           246. Defendant used the following items as a device or apparatus to intercept wire,  
 20 electronic, or oral communications made by Plaintiff and other Class Members:

21           a. The Website source code, which contained Tracking Tools that were used  
 22 to record and disseminate Plaintiff's and Class Members' communications as they used the  
 23 Website;

24           b. Plaintiff's and Class Members' browsers, which were commandeered and  
 25 manipulated by the Website's source code;

26           c. Plaintiff's and Class Members' computing and mobile devices;

e. Server-to-server communications between Defendant and Facebook and Defendant and Google which allowed the dissemination of Plaintiff's and Class Member's substantive communications without relying on third-party cookies.

247. Defendant failed to disclose its use of the Tracking Tools in the manner described herein, which specifically and automatically transmit the contents of Plaintiff's and Class Members communications to third parties for use in marketing.

248. To avoid liability under the FCSA, a defendant must show it had the consent of *all* parties to a communication.

249. The patient communication information that Defendant transmits via its Website, such as specific prescription information, constitutes protected health information.

250. As demonstrated above, Defendant violates the FCSA by aiding and permitting third parties to receive its patients' online communications in real time through its Website without their consent.

251. By disclosing Plaintiff's and Class Members' Sensitive Information, Defendant violated Plaintiff's and Class Members' statutorily protected privacy rights.

252. As a result of the above violations and pursuant to Florida Statutes, § 934.10, Plaintiff and Class Members are entitled to actual damages or liquidated damages of \$1,000 or \$100 per day for each violation, whichever is higher.

253. Under the statute, Defendant is also liable for reasonable attorneys' fees, reasonable litigation costs, injunctive and declaratory relief, and punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by the Defendant in the future.

## COUNT VIII

## Invasion of Privacy

**(By Plaintiffs and on behalf of the Nationwide Class)**

1           254. Plaintiffs reallege and incorporate by reference every allegation contained in the  
2 paragraphs above as though fully set forth herein.

3           255. Washington common law recognizes the tort of invasion of privacy. The right to  
4 privacy is also established in the Constitution of the State of Washington which explicitly  
5 recognizes an individual's right to privacy and states under Article 1, Section 7: "No person shall  
6 be disturbed in his private affairs, or his home invaded, without authority of law."

7           256. A claim for intrusion on seclusion requires (1) an intentional intrusion, physically  
8 or otherwise, (2) upon the solitude or seclusion of another or his private affairs or concerns, and  
9 (3) the intrusion must be highly offensive to a reasonable person.

10          257. Plaintiffs and the Class Members have an objective, reasonable expectation of  
11 privacy in browsing sessions conducted on their personal devices and their highly personal and  
12 private Sensitive Information, including their patient status, prescription and immunization  
13 information, health insurance information, and other highly sensitive data.

14          258. Defendant's conduct, through its unlawful embedding of Pixel and other Tracking  
15 Tools and subsequent interception, recording, and unauthorized disclosure of Plaintiffs' and the  
16 Class Members' private communications regarding sensitive health information when they  
17 visited and interacted with Defendant's Website without their consent, violates Article 1, Section  
18 7 of the Constitution of the State of Washington.

19          259. Plaintiffs and the Class Members did not consent to, authorize, or know about  
20 Defendant's intrusion at the time it occurred. Plaintiffs and the Class Members never agreed that  
21 Defendant could install a recording device (Pixel or other Tracking Tools) to actively record their  
22 Website Communications in real-time or disclose their private communications and sensitive  
23 health information to Defendant's vendors or other third parties.

24          260. Plaintiffs and the Class Members have a legitimate, objective, and reasonable  
25 expectation of privacy in private browsing sessions and precluding the dissemination and/or  
26 misuse of their highly sensitive health information and private communications and in

1 conducting their personal activities without intrusion or interference, including the right to not  
2 have their personal information intercepted and utilized for commercial gain.

3 261. By intentionally embedding and implementing the Tracking Tools on its Website,  
4 Defendant intruded upon, and permitted unauthorized third parties to intrude upon, Plaintiffs'  
5 and the Class Members' private communications with Defendant regarding their sensitive health  
6 information without consent.

7 262. Defendant's use of Pixel and other Tracking Tools also resulted in the publication  
8 of Plaintiffs and Class Members' private affairs to another in a manner that is highly offensive  
9 to a reasonable person. As a result of Defendant's use of the Tracking Tools, Plaintiffs' and Class  
10 Members sensitive health information was transmitted to the largest advertising companies in the  
11 world for purposes of creating targeted advertising and marketing campaigns.

12 263. Defendant's secret use of the Tracking Tools to record and disclose Plaintiffs' and  
13 the Class Members' Sensitive Information obtained via the Website is highly offensive and  
14 objectionable to a reasonable person and constitutes an egregious breach of the social norms  
15 underlying the right to privacy given the sensitive nature of the health information and state and  
16 federal statutes prohibiting disclosure of such information.

17 264. Defendant's conduct, by secretly and unlawfully intercepting, and permitting the  
18 unauthorized third-party use of, Plaintiffs' and the Class Members' communications any time  
19 they interacted with Defendant's Website with the Tracking Tools enabled without their consent,  
20 was a proximate cause of damage to Plaintiffs and the Class Members. Plaintiffs and the Class  
21 have suffered losses of privacy, loss of control of their private data, and a diminution of value of  
22 their personal information.

23 265. Additionally, given the monetary value of individual personal information,  
24 Defendant deprived Plaintiffs and the Class Members of the economic value of their interactions  
25 with Defendant's Website, without providing proper consideration for Plaintiffs' and the Class  
26 Members' property.

267. As a direct and proximate result of Defendant's conduct, Plaintiffs and the Class Members are entitled to damages, including compensatory, and/or nominal damages, in an amount to be proven at trial.

268. Plaintiffs re-allege and incorporate by reference every allegation contained in the paragraphs above as though fully stated herein.

270. An implicit part of the agreement was that Defendant would safeguard Plaintiffs' and Class Members' Sensitive Information consistent with industry and regulatory standards and Defendant's privacy policy and would timely notify Plaintiffs in the event of a disclosure to third parties.

272. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendant.

274. As a direct and proximate result of Defendant's breaches of these implied contracts, Plaintiffs and Class Members sustained damages as alleged herein. Plaintiffs and Class

Members would not have used Defendant's services, or would have paid substantially less for these services, had they known their sensitive health-related information would be disclosed.

275. Plaintiffs and Class Members are entitled to compensatory and consequential damages because of Defendant's breaches of implied contract.

### **COUNT X**

#### **Conversion**

#### **(By Plaintiffs and on behalf of the Nationwide Class)**

276. Plaintiffs reallege and incorporate by reference every allegation contained in the paragraphs above as though fully stated herein.

277. Plaintiffs and the Class Members provided their Sensitive Information to Defendant for the purposes of receiving healthcare services or healthcare-related information and knowledge. This Sensitive Information was the personal property of Plaintiffs and the Class Members.

278. Defendant converted Plaintiffs' and Class Members' Sensitive Information by willfully misappropriating and misusing the Sensitive Information for marketing purposes, which was not the intended purpose of Plaintiffs and Class Members in providing the personal information to Defendant.

279. Defendant's unlawful conversion interfered with and deprived Plaintiffs and Class Members of their possessory interests in their Sensitive Information by causing Plaintiffs and Class Members to lose control over the dissemination of their personal medical data, which was intended only for Defendant.

280. Plaintiffs' and Class Members' possessory rights in their Sensitive Information were seriously impaired by Defendant's intentional misuse and disclosure of their information to unauthorized third parties, from which Plaintiffs and Class Members have no ability recover their Sensitive Information.

281. As a direct and proximate result of Defendant's conversion, Plaintiffs and Class Members suffered the loss of their Sensitive Information and are entitled to damages, including compensatory and/or nominal damages, in an amount to be proven at trial.

### **COUNT XI**

#### **Unjust Enrichment (By Plaintiffs and on behalf of the Nationwide Class)**

282. Plaintiffs reallege and incorporate by reference every allegation contained in the paragraphs above as though fully stated herein.

283. Plaintiffs and the Class Members provided their Sensitive Information to Defendant for the purposes of receiving healthcare services or healthcare-related information and knowledge. Defendant knowingly and unlawfully received a benefit from its use of Plaintiffs' and the Class Members' Sensitive Information, including monetary compensation. Defendant intentionally and knowingly collected and used Plaintiffs' and the Class Members' Sensitive Information for its own gain, without Plaintiffs' or the Class Members' consent, authorization, or compensation.

284. Defendant unjustly retained those benefits and enriched itself at the expense of Plaintiffs and the Class Members, and this conduct damaged Plaintiffs and the Class Members. Plaintiffs and the Class Members were not compensated by Defendant for the data they unknowingly provided.

285. It would be inequitable and unjust for Defendant to retain any of the profit or other financial benefits derived from the secret, unfair, and deceptive data harvesting methods Defendant employs on its Website.

286. The Court should require Defendant to disgorge all unlawful or inequitable proceeds that it received into a common fund for the benefit of Plaintiffs and the Class Members, and order other such relief as the Court may deem just and proper.

287. Plaintiffs allege this claim in the alternative in the event Plaintiffs and Class Members have an inadequate remedy at law.

**REQUEST FOR RELIEF**

WHEREFORE, Plaintiffs respectfully pray for judgment in their favor as follows:

- a. Certification of the Class pursuant to the provisions of Fed. R. Civ. P. 23 and an order that notice be provided to all Class Members;
- b. Designation of Plaintiffs as representatives of the Class and the undersigned counsel as Class Counsel;
- c. An award of damages in an amount to be determined at trial or by this Court;
- d. Declaring that Defendant's past conduct was unlawful, as alleged herein;
- e. Declaring Defendant's ongoing conduct is unlawful, as alleged herein;
- f. Enjoining Defendant from continuing the unlawful practices described herein, and awarding such injunctive and other equitable relief as the Court deems just and proper;
- g. Awarding Plaintiffs and the Class Members statutory, actual, compensatory, consequential, and nominal damages, as well as restitution and/or disgorgement of profits unlawfully obtained;
- h. Awarding Plaintiffs and the Class Members pre-judgment and post-judgment interest;
- i. Awarding Plaintiffs and the Class Members reasonable attorneys' fees, costs, and expenses; and
- j. Granting such other relief as the Court deems just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiffs, on behalf of themselves and the Class, demand a trial by jury of any and all issues in this action so triable of right.

1 DATED this 26th day of January, 2024.

2 **TOUSLEY BRAIN STEPHENS PLLC**

3  
4 By: s/ Kim D. Stephens, P.S.  
Kim D. Stephens, P.S., WSBA #11984  
5 By: s/ Rebecca L. Solomon  
Rebecca L. Solomon, WSBA #51520  
6 1200 Fifth Avenue, Suite 1700  
Seattle, WA 98101  
7 Telephone: (206) 682-5600  
Facsimile: (206) 682-2992  
8 kstephens@tousley.com  
9 rsolomon@tousley.com

10 **ZIMMERMAN REED LLP**

11 By: s/Hart L. Robinovitch  
12 Hart L. Robinovitch (*admitted pro hac vice*)  
Ryan J. Ellersick, WSBA # 43346  
13 14648 North Scottsdale Road, Suite 130  
Scottsdale, AZ 85254  
14 Telephone: (480) 348-6400  
hart.robinovitch@zimmreed.com  
15 ryan.ellersick@zimmreed.com

16 **MILBERG COLEMAN BRYSON PHILLIPS**  
17 **GROSSMAN, PLLC**

18 Gary M. Klinger (*admitted pro hac vice*)  
227 W. Monroe Street, Suite 2100  
19 Chicago, IL 60606  
Telephone: (866) 252-0878  
20 gklinger@milberg.com

21 Glen L. Abramson (*admitted pro hac vice*)  
Alexandra M. Honeycutt (*admitted pro hac vice*)  
22 800 S. Gay Street, Suite 1100  
Knoxville, TN 37929  
23 Telephone: (866) 252-0878  
gabramson@milberg.com  
24 ahoneycutt@milberg.com

**BARRACK RODOS & BACINE**

Stephen R. Bassar (*admitted pro hac vice*)

sbassar@barrack.com

Samuel M. Ward (*admitted pro hac vice*)

sward@barrack.com

600 West Broadway, Suite 900

San Diego, CA 92101

Telephone: (619) 230-0800

**LEVI & KORSINSKY, LLP**

Mark S. Reich\*

Courtney Maccarone\*

mreich@zlk.com

cmaccarone@zlk.com

33 Whitehall Street, 17<sup>th</sup> Floor

New York, NY 10004

Telephone: 212-363-7500

Fax: 212-363-7171

*\*Pro Hac Vice applications to be submitted*

*Attorneys for Plaintiffs and the Putative Class*